ANÁLISIS DE RIESGOS INFORMÁTICOS Y SUGERENCIA DE CONTROLES PARA LA MITIGACIÓN DEL RIESGO EMPLEANDO LAS NORMAS ISO/IEC 27001, ISO/IEC 27002 E ISO/IEC 27005 SOBRE LOS ACTIVOS CRÍTICOS DE T.I. EN LA SEDE ADMINISTRATIVA DE LA EMPRESA MODANOVA S.A.S.

FERNANDO CASTIBLANCO
LUIS ALEXANDER OVIEDO REGUEROS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

ANÁLISIS DE RIESGOS INFORMÁTICOS Y SUGERENCIA DE CONTROLES PARA LA MITIGACIÓN DEL RIESGO EMPLEANDO LAS NORMAS ISO/IEC 27001, ISO/IEC 27002 E ISO/IEC 27005 SOBRE LOS ACTIVOS CRÍTICOS DE T.I. EN LA SEDE ADMINISTRATIVA DE LA EMPRESA MODANOVA S.A.S.

FERNANDO CASTIBLANCO
LUIS ALEXANDER OVIEDO REGUEROS

PROYECTO DE GRADO PARA OPTAR AL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
ING. JUAN CARLOS ALARCÓN SUESCÚN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2016

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Piloto de Colombia para optar al título de Especialista en Seguridad Informática.

_____

Firma Presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 16 de noviembre de 2016

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE GRÁFICOS

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVOS[1]: los activos a nivel tecnológico, son todos los relacionados con los sistemas de información, las redes y comunicaciones y la información en sí misma. Por ejemplo, los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros.

ADMINISTRACION DE PARCHES[2]: Una política de aplicación de parches determina la estrategia, procedimientos y requisitos en la actualización del software de los sistemas de información. Es una parte más de los procedimientos de gestión del riesgo de las organizaciones, en este caso orientado a dar respuesta inmediata al descubrimiento de problemas, vulnerabilidades o debilidades de los sistemas de comunicaciones o pro cesamiento de la información.

AMENAZAS[3]: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en las operaciones de la organización, comúnmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas pueden ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos.

DNS[4]: del inglés (Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa. Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar (pero que también pueden causar muchos conflictos, puesto que los nombres son activos valiosos en algunos casos).

---

[1] UNIVERSIDAD NACIONAL UNAD. Lección 3 Análisis De Riesgos, Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_3_anlisis_de_riesgos.html, [Citado en 31/07/2016].

[2] UNIVERSIDAD AUTONOMA DE BUCARAMANGA, Mitigación De Riesgos, Disponible en: http://wlserver.unab.edu.co/portal/page/portal/UNAB/apoyo-a-la-academia/servicios/seguridadinformatica/descargas/otros/GESTION_DE_PARCHES_NO.PDF, [Citado en 15/02/2017].

[3] UNIVERSIDAD DE LA REPUBLICA URUGUAY. Introducción al riesgo informático, Pagina 3, Disponible en: http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf, [Citado en 30/10/2016].

[4] UNIVERSIDAD DE CHILE, Definición de sigla dns, Disponible en: http://users.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html, [Citado en 05/01/2017].

DIRECCIÓN IP[5]: para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión, este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) de pendiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bites. la dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.

HARDENING[6]: configurar una computadora u otros dispositivos de red para resistir ataques.

IMPACTOS[7]: son las consecuencias de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financiaras, económicas, tecnológicas, físicas, entre otras.

INFORMACIÓN[8]: es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno, que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

NORMA ISO 27001[9]: la norma ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

SUBCONTRATACION[10]: La subcontratación es proceso empresarial mediante el cual una sociedad transfiere la responsabilidad de sus tareas externas a otra sociedad especializada en esa tarea. La empresa subcontratada es aquella que mediante un acuerdo con otra empresa (a la que suele llamarse contratista o cliente) lleva a cabo la realización de determinadas actividades y servicios. El modo en el

---

[5] HERRAMIENTAS WEB, Definición de sigla ip, Disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html, [Citado en 05/01/2017].

[6] ISACA. Glossary of Terms, Disponible en: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf, [Citado en 31/07/2016].

[7] UNIVERSIDAD NACIONAL UNAD. Lección 3 Análisis De Riesgos, Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_3_anlisis_de_riesgos.html, [Citado en 31/07/2016].

[8] DATOSUNO. Introducción a la informática, Disponible en: https://datosuno.wordpress.com/unidad-1/introduccion/ , [Citado en 25/08/2016].

[9] 27001 ACADEMY, ¿Qué es la norma 27001?, Disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/, [Citado en 15/10/2016].

[10] ECONOMIPEDIA, Definición de termino subcontratación, Disponible en: http://economipedia.com/definiciones/subcontratacion.html, [Citado en 25/08/2016].

que esta relación comercial se desarrolla suele estar definido previamente mediante un contrato.

POLÍTICAS[11]**:** son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias.

POLÍTICAS DE SEGURIDAD EN LA INFORMACIÓN[12]**:** comprenden un conjunto de reglas a ser aplicadas a todas las actividades relacionadas con los sistemas de información que soportan los procesos críticos de la empresa con el objeto de garantizar la integridad, confidencialidad y disponibilidad de la información.

PROBABILIDAD[13]**:** la probabilidad es la mayor o menor posibilidad de que ocurra un determinado suceso. En otras palabras, su noción viene de la necesidad de medir o determinar cuantitativamente la certeza o duda de que un suceso dado ocurra o no.

POODLE[14]**:** el ataque POODLE (del inglés "Padding Oracle On Downgraded Legacy Encryption") es un exploit man-in-the-middle que aprovecha Internet y la característica del software de clientes de bajar a SSL 3.0.1 2 3, Si los atacantes explotan exitosamente esta vulnerabilidad, en promedio, solo necesitan hacer 256 solicitudes SSL 3.0 para revelar un byte de los mensajes cifrados.

SGSI[15]**:** es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

---

[11] GESTIOPOLIS.COM, Política organizacional. Concepto y esquema en la empresa, Disponible en: http://www.gestiopolis.com/politica-organizacional-concepto-y-esquema-en-la-empresa/, [Citado en 05/09/2016].

[12] SEGUINFO, Políticas de seguridad de la información, Disponible en: http://www.segu-info.com.ar/politicas/polseginf.htm , [Citado en 20/08/2016].

[13] CONCEPTODEFINICION.DE, Ciencia P. Definición de probabilidad, Disponible en: http://conceptodefinicion.de/probabilidad/ , [Citado en 18/09/2016].

[14] WELIVE SECURITY, Definición de ataque poodle, Disponible en: http://www.welivesecurity.com/la-es/2014/10/15/poodle-vulnerabilidad-ssl-3/, [Citado en 30/12/2016].

[15] ISO 27000.ES, Definición de sigla SGSI, Disponible en: http://www.iso27000.es/sgsi.html, [Citado en 05/01/2017].

SEGURIDAD INFORMÁTICA[16]: la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

VULNERABILIDADES[17]: son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevando a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

VLAN[18]: es una (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

[16] SOL-IT SEGURIDAD INFORMÁTICA, Objetivos de la seguridad informática, Disponible en: http://sol-it.com.co/seguridad-informatica/ , [Citado en 30/09/2016].

[17]UNIVERSIDAD DE LA REPUBLICA URUGUAY, Introducción al riesgo informático, Pagina 3, Disponible en: http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf, [Citado en 30/10/2016].

[18] VLAN REDES VIRTUALES, Definición de sigla vlan, Disponible en: http://es.ccm.net/contents/286-vlan-redes-virtuales, [Citado en 05/01/2017].

RESUMEN

En el presente proyecto se realizó un análisis de riesgos informáticos para los procesos críticos de la empresa MODANOVA S.A.S en donde surgieron controles para mitigar los riesgos identificados empleando las normas ISO/IEC 27001, ISO/IEC 27002 E ISO/IEC 27005 sobre los activos críticos de T.I. en la sede administrativa de la citada empresa.

Se desarrolló el proyecto aplicando la norma ISO/IEC 27001:2013 creando cuadros para levantamiento de información, análisis, valoraciones y un análisis minucioso de los procesos críticos de generación, transporte y almacenamiento de información, con el fin de realizar una evaluación de riesgos al software que se encarga de administrar o proteger la información importante para MODANOVA.

Al final del proceso se realizó un cuadro de actividades recomendadas con el fin de mitigar los riesgos encontrados y así evitar posibles pérdidas, daños o hurto de información en los procesos críticos en MODANOVA S.A.S.

Al finalizar de este proyecto se entregará a MODANOVA. S.A.S un documento con los riesgos encontrados, su respectiva evaluación y la recomendación de cómo solventar o mitigar estos riesgos con el fin de evitar que se vean afectados los 3 aspectos de la información (Confidencialidad, Integridad y Disponibilidad).

PALABRAS CLAVE: INGENIERÍA DE SISTEMAS. T.I.ISO/IEC 27000. ISO/IEC 27001. ISO/IEC 27002. ISO/IEC 27003. ISO/IEC 27005. ACTIVOS. RIESGOS. VULNERABILIDADES.

INTRODUCCIÓN

MODANOVA S.A.S es una empresa con carácter comercial en donde sus procesos misionales se apoyan en la tecnología; tales como administrativos, financieros, producción y ventas. Actualmente la empresa se encuentra en una etapa de expansión, mejora de procesos, búsqueda de nuevos mercados, nuevos canales de venta, crecimiento en infraestructura y posicionamiento de la marca Brissa (Marca de MODANOVA S.A.S.).

Los sistemas de información son uno de los activos más importantes de las organizaciones, pero no toda la información, ni todos los sistemas tienen la misma importancia ni criticidad para las empresas. Por ello la prioridad al momento de hacer inversiones es mayor sobre los sistemas de información enfocados al logro de los objetivos misionales de la empresa.

La información se puede preservar, consultar y analizar, manteniendo e implementando unos adecuados controles y políticas para registro y manipulación en los sistemas informáticos.

Naturalmente la tecnología ayuda a cumplir la misión de las empresas, incrementando la velocidad, eficiencia y eficacia de los procesos, así como la facilidad de interactuar con más mercados e incrementar ganancias, pero estas ventajas ocasionan dependencia de la tecnología y exposición a los riesgos de la tecnología.

Para lograr la seguridad de la información, se debe garantizar que se cumple con los tres (3) pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Al definir correctamente activos críticos, procesos y controles para garantizar estos tres objetivos se proveerá un alto nivel de protección sobre la información.

Un grave error que cometen las organizaciones y algunos ingenieros, es creer que existe seguridad al evitar revelar información sobre los sistemas; que entre menos conozcan del mismo, más seguro estará, y esto es falso. Con el simple hecho de tener sistemas de información, sea automatizado o manual, estos poseen vulnerabilidades inherentes a la naturaleza del mismo y por ende existen riesgos dada la importancia de la información manipulada, la posición, los privilegios o ubicación del sistema en la empresa.

La empresa MODANOVA S.A.S. no posee área de seguridad informática o de la información, y en el pasado se ha visto afectada por problemas de seguridad informática, tales como virus, indisponibilidades y fraudes bancarios que según la entidad bancaria asociada a MODANOVA S.A.S. han sido efectuados desde la misma empresa, pero nunca fue identificado el procedimiento efectuado o las falencias especificas existentes en MODANOVA S.A.S. que han permitido estos fraudes. Peor aún, es que se desconoce si existen más fraudes no descubiertos o que tanto ha sido comprometida la seguridad informática de MODANOVA S.A.S.

El presente proyecto contribuirá en la protección de la información de los procesos críticos de almacenes MODANOVA S.A. realizando análisis de riesgos mediante las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 y sugiriendo acciones de mejora que ayuden a mitigar los riesgos.

MODANOVA S.A. estará muy beneficiada por este proyecto, ya que no necesitará contratar un experto en seguridad informática, ni crear un área de seguridad, ni invertir grandes sumas de dinero en herramientas o infraestructura de seguridad, ya que contará con el apoyo de los ingenieros que desarrollan el presente proyecto para que con sus conocimientos en seguridad identifiquen activos, niveles de criticidad, amenazas, riesgos, vulnerabilidades, controles y sugieran acciones de mejora. La empresa habrá ahorrado millones de pesos por este trabajo y podrá tener documentadas sus falencias y riesgos informáticos para iniciar acciones de remediación de riesgos de seguridad de la información para sus procesos críticos.

El proyecto permite sentar los puntos de partida para iniciar el proceso de certificación en ISO 27001:2013. No se hará compra o uso de software o herramientas propietarias cuyo uso conlleve a adquisición formal de las mismas; en su lugar se emplearán herramientas de uso libre que ayuden a contribuir con los objetivos del proyecto.

Adicionalmente este proyecto de grado servirá de referencia o guía a otros estudiantes de la Universidad Piloto de Colombia, de cómo se realiza un análisis de riesgos utilizando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 en una empresa real, qué elementos evaluar en una empresa en donde no existe sistema de gestión de seguridad de la información y como recomendar acciones de mejora.

1. PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo identificar riesgos informáticos y sugerir controles para la mitigación del riesgo empleando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 sobre los activos críticos de T.I. en la sede administrativa de la empresa MODANOVA S.A.S.?

1.2 JUSTIFICACIÓN

MODANOVA S.A.S. se ha visto afectada por problemas de seguridad informática, tales como virus, indisponibilidades y fraudes bancarios que según la entidad bancaria asociada a MODANOVA S.A.S. han sido efectuados desde la misma empresa, pero nunca fue identificado el procedimiento efectuado o las falencias especificas existentes en MODANOVA S.A.S. que han permitido estos fraudes. Peor aún, es que se desconoce si existen más fraudes no descubiertos o que tanto ha sido comprometida la seguridad informática de MODANOVA S.A.S.

Actualmente las empresas y organizaciones medianas como MODANOVA S.A.S. deben considerar dentro de sus planes de gobierno y negocio el aseguramiento de la información generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia.

MODANOVA S.A.S. ha establecido como política corporativa alinear sus objetivos institucionales y misionales a la seguridad informática en sus procesos para proteger el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma, para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información como un primer paso y realizar las recomendaciones que de este análisis se deriven para que en un futuro sirva de base para implementar el sistema de gestión de seguridad de la información (SGSI), que permitirá mantener un modelo de negocio estable logrando un valor agregado y posicionamiento en el mercado de artículos de decoración.

Al realizar este análisis de riesgos informáticos, MODANOVA S.A.S.se beneficia inmediatamente por identificar sus fortalezas y debilidades en seguridad informática, recibiendo adicionalmente las recomendaciones para fortalecerse y poder proteger de manera adecuada sus activos informáticos críticos.
Al aplicar las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC en 27005 en el análisis de riesgos, se proporcionará a MODANOVA S.A.S la base para poder crear

un departamento de seguridad de la información, identificar debilidades en los activos información críticos e incluso poder llegar a certificarse en ISO 27001.

1.3 OBJETIVO GENERAL

Realizar un análisis de riesgos informáticos y sugerir controles para la mitigación delos riesgos empleando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 sobre los activos críticos de T.I. en la sede administrativa de la empresa MODANOVA S.A.S.

1.4 OBJETIVOS ESPECÍFICOS

- Realizar inventario de los activos críticos de T.I. en la sede administrativa de la empresa MODANOVA S.A.S.
- Identificar los procesos críticos de generación, proceso y almacenamiento de información.
- Realizar un inventario de software instalado en equipos informáticos que involucran el manejo de la información crítica en la empresa.
- Realizar un análisis de vulnerabilidades utilizando herramientas tecnológicas de detección y verificación sobre los activos críticos de la compañía.
- Identificar amenazas que puedan explotar o aprovechar las vulnerabilidades encontradas en los activos críticos de T.I.
- Evaluar riesgos a los que están expuestos los activos críticos de T.I. de MODANOVA S.A.S.
- Sugerir controles que minimicen los riesgos de acuerdo con sus criticidades.
- Elaborar informe de riesgos encontrados, niveles de exposición y acciones de mejora recomendadas dirigidas a la alta gerencia.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

MODANOVA S.A.S. es una empresa colombiana con una trayectoria de 20 años, cuya misión es elaborar y comercializar productos para el hogar orientados a cumplir con los parámetros de calidad, diseño y tendencias que se ajusten a las normas internacionales y que satisfagan las necesidades y expectativas de los clientes.

“Brissa cosas de casa” es una marca exclusiva de MODANOVA S.A.S., que nace en el año 1992 comercializa productos textiles que inicialmente eran básicos para el hogar y con el tiempo fueron aumentando, no sólo en variedad, sino también en diseño. Adicionalmente, la compañía que inicia produciendo y adquiriendo los productos nacionalmente, se extiende en el campo de las importaciones, la venta al por mayor y por catálogo, siempre teniendo en cuenta las últimas tendencias de la moda en el hogar.

MODANOVA S.A.S. en su crecimiento constante y expansión, ha implementado diferentes procesos y estrategias de negocio las cuales en su mayoría se soportan en la tecnología de información, en esta trayectoria se han presentado algunos eventos que han revelado la necesidad de asegurar y mejorar sus procesos de seguridad de la información a nivel administrativo, por lo cual necesita identificar riesgos informáticos en su sede principal para sus activos de información más importantes con el fin de mejorar sus procesos internos en el tratamiento de la información.

2.2 MARCO GEOGRÁFICO

MODANOVA S.A.S tiene sus oficinas principales ubicadas en la carrera 62 # 10–40 en la ciudad de Bogotá y se puede apreciar la oficina principal en la Ilustración 1. Oficina principal almacenes Brissa. En esta sede se encuentran las áreas de gerencia, comercial, diseño, espacios comerciales, sistemas, contabilidad, nómina y RR.HH.

Ilustración 1.Oficina principal almacenes brissa

Fuente. Archivo fotográfico MODANOVA S.A.S.

En la Ilustración 2. Planta de producción MODANOVA S.A.S. SIBATÉ, e Ilustración 3. Planta de producción MODANOVA S.A.S. SIBATÉ, se observan la planta de producción ubicada en Sibaté- Cundinamarca Km 4 vía Sibaté, que cuenta con las áreas de compras, producción, costos, planeación y mantenimiento.

Ilustración 2.Planta de producción modanova

Fuente. Archivo fotográfico MODANOVA S.A.S.

Ilustración 3.Planta de producción modanova

Fuente. Archivo fotográfico MODANOVA S.A.S.

MODANOVAS.A.S. cuenta también con 21 tiendas Brissa ubicadas a nivel nacional. Una de las más populares es el almacén Brissa del centro comercial Unicentro que puede apreciarse en la Ilustración 4. Almacén Brissa Unicentro Bogotá.

Ilustración 4. Almacén brissa unicentro bogotá

Fuente. Archivo fotográfico MODANOVA S.A.S.

En el Cuadro 1. Ubicaciones almacenes Brissa, se muestran las diferentes ubicaciones de las tiendas almacenes Brissa de MODANOVA S.A.S.

Cuadro 1. Ubicaciones almacenes brissa

Ciudad	Almacén	Dirección	Teléfono
Bogotá	Brissa Outlet fábrica	Avenida 9 # 60 - 70 loc 15 y 16	4200620
Bogotá	Brissa Cafam Floresta	Cra 48F # 96-50 local 126	5340843
Bogotá	Brissa Unicentro	Cra 15 # 123 -30 local 152	2130995
Bogotá	Brissa Plaza de las américas	Transversal 71 D # 6 - 94 Local 1401	4137469
Bogotá	Brissa Salitre plaza	Cra 68B # 24 - 39 Local 261	4169209
Bogotá	Brissa Atlantis	Calle 80 # 13 - 06 local 305	6108457
Bogotá	Brissa Palatino	Cra 7 # 139 - 7 Local 218	6146165
Bogotá	Brissa Unicentro de Occidente	Cra 111c # 86 - 74 local 131	4405366
Bogotá	Brissa Santafé	Calle 184 # 46 - 96 local 105	7012212
Bogotá	Brissa Outlet Floresta	Carrera 49A # 99 - 49 Bodega 1	6130161
Bogotá	Brissa Hayuelos	Calle 20 # 82 - 52 Local 167	3546098
Chía	Brissa Chía	Avenida Pradilla # 9 - 00 Este	8707308
Cartagena	Brissa Caribe	Calle 29D # 22 - 62 Local 1-85	6720602
Bucaramanga	Brissa Megamall	Av. Quebrada seca 33A - 100 Local 223	6326494
Bucaramanga	Brissa Cabecera	Cra 38C # 49 - 51 Local 203-II	6430241
Montería	Brissa Alamedas	Calle 44 # 10 - 91 local 122B	7852438
Cali	Brissa Chipichape	Calle 38 Norte Av. 6 norte 35 Local 519A	6838215
Cali	Brissa Palmetto	Calle 9 # 49 - 50 Local 112	5137494
Barranquilla	Brissa Buenavista	Cra 53 # 98 - 99 Local 224	3579190
Santa Martha	Brissa Santa Martha	Calle 14 # 34 - 1 Local 49	4338899
Villavicencio	Brissa Villavicencio	Av. 40 # 33 - 00 Local 221	6653905
Pereira	Brissa Pereira	Calle 15 # 13 - 136 Local 174	3390111

Fuente. Elaborado por los autores.

Para efectos de la realización de este proyecto, el análisis se centra en la oficina principal de Bogotá, carrera 62 # 10-40.

2.3 MARCO CONCEPTUAL

La información es uno de los principales activos de las organizaciones. La defensa de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, así como también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además traslada confianza a los clientes y/o usuarios.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

Los sistemas de gestión de seguridad de la información son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus

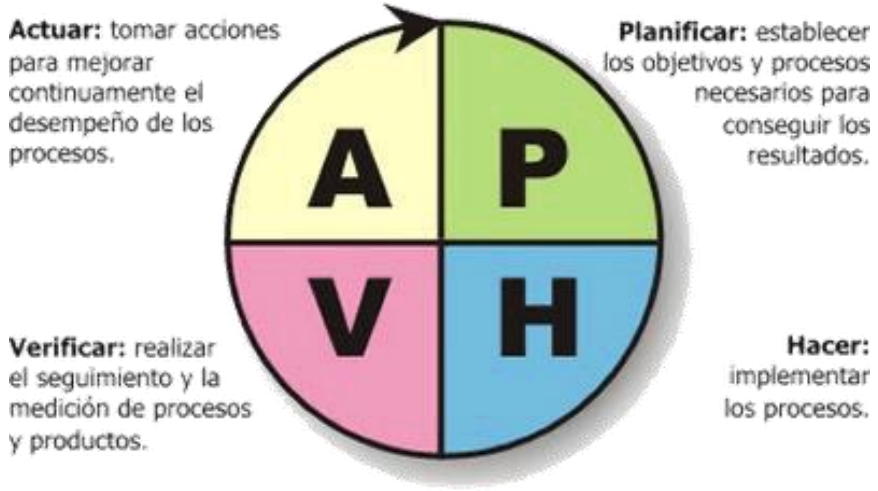
riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio.

Una gestión eficaz de la seguridad de la información permite garantizar: Confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información. Integridad, asegurando que la información y sus métodos de proceso son exactos y completos. Y disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La implantación de un SGSI se basa en la norma NTC ISO/IEC 27001:2013. Esta norma presenta un sistema de gestión basado en el ciclo de Deming: Plan, Do, Check, Act, conocido como PDCA y que traducido al castellano sería Planificar, Hacer, Verificar y Actuar (PHVA). El ciclo supone la implantación de un sistema de mejora continua que requiere una constante evolución para adaptarse a los cambios producidos en su ámbito y para tratar de conseguir la máxima eficacia operativa.

En el Gráfico 1. Ciclo PHVA, se pueden apreciar a grandes rasgos las etapas del ciclo PHVA o PDCA (siglas en inglés).

Gráfico 1. Ciclo PHVA



Fuente: http://www.totalqualidade.com.br/2012/09/herramientas-de-calidad-el-ciclo-phva.html

A continuación, se describe un poco acerca del funcionamiento del ciclo PDCA o PHVA:[19]

[19] AUDISEC.ES. Guía de implantación de un sistema de gestión de seguridad de la información une – iso/iec 27001:2007 con la herramienta Global SGSI, Disponible En: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf, [Citado En:31/07/2016]

2.3.1 Planificar. En esta fase tiene lugar la creación del SGSI, con la definición del alcance y la política de seguridad. El núcleo fundamental de esta fase y del SGSI es la realización de un análisis de riesgos que refleje la situación actual de MODANOVA S.A.S. A partir del resultado de este análisis se define un plan de tratamiento de riesgos que conlleve la implantación en la organización de una serie de controles de seguridad con el objetivo de mitigar los riesgos no asumidos por la dirección.

2.3.2 Hacer. Esta fase cubre la implantación del plan de tratamiento de riesgos y su ejecución. Incluye también la formación y concienciación de los empleados en materia de seguridad y la definición de métricas e indicadores que sirvan para evaluar la eficacia de los controles implantados.

2.3.3 Verificar. Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema. Entre ellos, se realiza una auditoría interna independiente y objetiva, así como una revisión global del SGSI por dirección con el objetivo de determinar nuevas metas a cubrir en el próximo ciclo del SGSI.

2.3.1 Actuar. El resultado de las revisiones debe reflejarse en la definición e implantación de acciones correctivas, preventivas y de mejora para avanzar en la consecución de un SGSI eficaz y eficiente.

[20]En el contexto de la seguridad y en términos del estándar ISO 27001, un riesgo puede ser expresado como el efecto de la incertidumbre sobre los objetivos de seguridad de la información. También, está asociado a la causa potencial de que una amenaza pueda explotar una o más vulnerabilidades de un activo o grupo de activos de información, teniendo como consecuencia algún tipo de daño.

Generalmente, los riesgos se expresan en términos de la combinación de la posibilidad de ocurrencia de un evento no deseado (probabilidad) y sus consecuencias (impacto), por lo que las medidas de seguridad están orientadas a reducir alguna de estas dos variables, o en el mejor de los casos a ambas.

La identificación de riesgos pretende conocer los activos más importantes para una organización junto con las amenazas que podrían afectarlos. Posteriormente, el análisis de los riesgos permite caracterizar cada uno de ellos para luego ser evaluados de forma cualitativa o cuantitativa en función de los criterios definidos por la organización. Todo esto se considera dentro de la fase de valoración.

[20]WELIVE SECURITY. De la identificación y análisis a la gestión de riesgos de seguridad, Disponible En: http://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/, [Citado En:31/07/2016]

Una vez que los riesgos han sido evaluados y priorizados (valorados en su conjunto), la siguiente fase tiene como propósito llevar a cabo actividades para su tratamiento: mitigar, eliminar, transferir o aceptar. Esta etapa tiene como objetivo la definición de las acciones a realizar con relación a los riesgos y la aplicación de controles de seguridad.

2.3.5 Mitigar. Es la ejecución de medidas de intervención dirigidas a reducir o disminuir el riesgo existente. La mitigación asume que en muchas circunstancias no es posible, ni factible, controlar totalmente el riesgo existente; es decir, que en muchos casos no es posible impedir o evitar totalmente los daños y sus consecuencias, sino más bien reducirlos a niveles aceptables y factibles. La mitigación de riesgos de desastre puede operar en el contexto de la reducción o eliminación de riesgos existentes, o aceptar estos riesgos y a través delos preparativos, los sistemas de alerta, entre otros, buscar disminuirlas pérdidas y daños que ocurrirían con la incidencia de un fenómeno peligroso.

2.3.6 Transferir. La transferencia del riesgo consiste en trasladar el riesgo a otros, ya sea vendiendo el activo riesgoso o comprando una póliza de seguros; se traspasa el riesgo a otra compañía (subcontratación, póliza de seguro), es importante recalcar la importancia del método de transferencia del riesgo, ya que hoy en día es el método más utilizado en la administración de riesgos, a su vez, es el método al que se recurre a través de instrumentos derivados.

2.3.7 Aceptar. Se presenta cuando el impacto es suficientemente bajo para que la organización decida no tomar ninguna acción de mitigación o cuando el costo de la aplicación de un control supera el valor del activo, la eliminación es una actividad ideal, ya que difícilmente se puede reducir a cero un riesgo y generalmente se presenta cuando el activo en cuestión deja de tener valor, por lo que los riesgos asociados pueden ser descartados, cuando se ha definido una acción para cada riesgo valorado, es necesario que los resultados sean aceptados y las medidas de seguridad aplicadas. Esto se vuelve necesario ya que, al aplicar una contramedida o control, todavía se cuenta con un riesgo denominado residual, es decir, un remanente que debe ser aprobado.

2.4 APLICABILIDAD NORMA ISO 27001

La Información es un activo fundamental para el desarrollo, operatividad, control y gestión del modelo de negocio / servicio de cualquier organización.

A través de los sistemas de información se canalizan prácticamente la totalidad de las actividades corporativas, desde sus aspectos operativos hasta las decisiones gerenciales, siendo estos sistemas elementos clave en el gobierno corporativo de dichas organizaciones, sea cual sea su tamaño y sector.

La seguridad de la información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel. En los entornos globalizados actuales, donde las transacciones de negocio de MODANOVA S.A.S. llevan en su praxis el sufijo “electrónico”, esta prioridad se maximiza ante las especiales características del medio en que se desarrollan y sus riesgos asociados.

Estas actividades derivan en la existencia de una serie de normas estándares, aceptadas como acreditaciones de la seguridad de la información universalmente, y cuya implementación aportaría a MODANOVA S.A.S no solo una certificación reconocida sino, como punto fundamental, una cultura y práctica de la seguridad que le aporta valores al negocio / servicio en muy diferentes aspectos así:

- Mejora de la competitividad
- Mejora de la imagen corporativa
- Protección y continuidad del negocio
- Cumplimiento legal y reglamentario
- Optimización de recursos e inversión en tecnología
- Reducción de costes

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un sistema de gestión de la seguridad de la información (SGSI).

Entre las actividades propias a desarrollar al abordar una implantación a ISO27001 se encuentran:

- Definición del alcance del SGSI
- Definición de una Política de Seguridad
- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
- Identificación de riesgos
- Evaluación de los posibles tratamientos del riesgo
- Elaboración de un Declaración de Aplicabilidad de controles y requisitos
- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias

- Elaboración de procedimientos y documentación asociada

Como otras normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad. Asimismo, está basada en un enfoque por procesos y en la mejora continua, por lo tanto, es perfectamente aplicable, compatible e integrable con el resto de sistemas de gestión que ya existan en MODANOVA S.A.S.

3. DISEÑO METODOLÓGICO

En el Gráfico 2. Identificación de riesgos informáticos, se muestran los pasos ejecutados para la identificación, análisis, evaluación y remediación de los riesgos informáticos de los activos críticos de T.I. con base en NTC-ISO/IEC 27005.

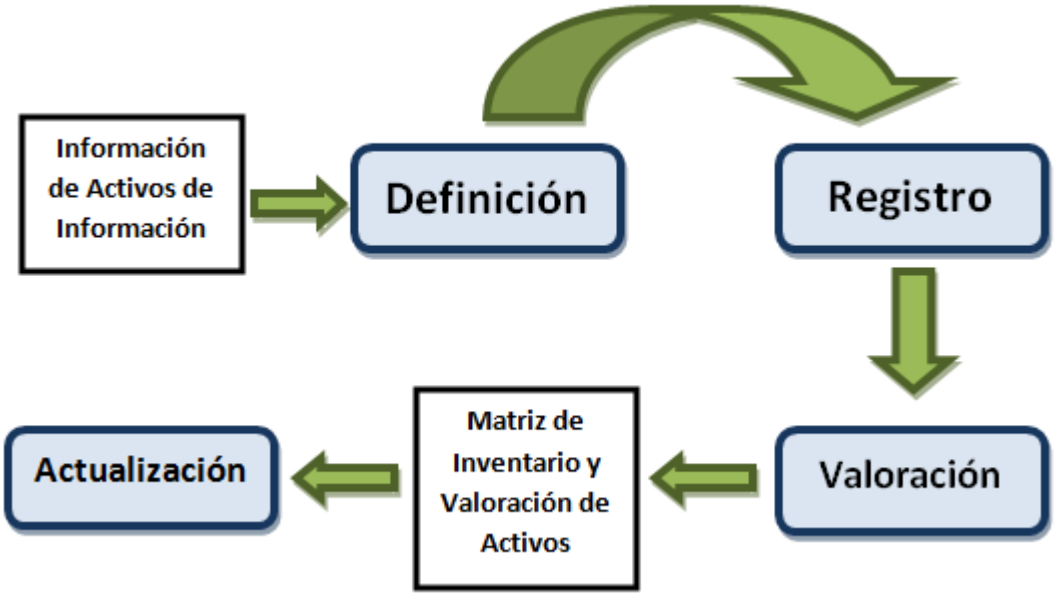
Gráfico 2. Identificación de riesgos informáticos

Fuente. Elaborado por los autores.

3.1 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS DE T.I.

Para identificar los activos críticos de T.I. se diseñó el proceso: información de activos de información, definición, registro, valoración, matriz de inventario y valoración de activos y finalmente actualización, como se describe en el Gráfico 3. Realización de inventario de activos críticos de T.I.

Gráfico 3. Realización de inventario de activos críticos de T.I.



Fuente. Elaborado por los autores.

3.1.1 Información de activos de información. La definición del inventario de activos es prerrequisito de la gestión de riesgos, pues permite identificar aquellos activos de T.I. a los que se les debe brindar mayor protección al ser vitales para la ejecución de los procesos y prestación de los servicios, y requieren niveles altos de integridad, confidencialidad y disponibilidad. Contar con un registro de inventario de activos clasificados persigue dar cumplimiento a tres puntos principales de la norma NTC ISO/IEC 27001:2013 respecto a la “Gestión de Activos”.

3.1.1.1Inventario de activos. Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de los mismos dentro de la organización.

3.1.1.2Propiedad de los activos. Toda la información y los activos asociados con los servicios de procesamiento de información deben ser “propiedad” de una parte designada de la organización.

3.1.2 Definición. La definición consiste en determinar qué activos de información van a hacer parte del inventario e identificar sus propiedades, los cuales se muestran en el Cuadro 2. Listado de activos críticos de MODANOVA S.A.S.

3.1.2.1 Directrices de clasificación. La información debe clasificarse en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

3.1.3 Registro. Se registra la información reunida hasta el momento con sus definiciones como se observa en el Cuadro 2. Listado de activos críticos de MODANOVA S.A.S.

Cuadro 2. Listado de activos críticos de modanova

Consecutivo	Proceso	Procedimiento	Activo	Descripción	Formato
1	CONTABILIDAD GENERAL, FACTURACIÓN, CARTERA, INVENTARIOS, COSTOS Y PRODUCCIÓN	Control de contabilidad, planeación, inventarios, costos y producción	Servidor de aplicación ERP	Equipo servidor HP ML 350 G6, asignado para la ejecución de programa ERP - Priority	FÍSICO
2	CONSOLIDACIÓN Y ALMACENAMIENTO DE INFORMACIÓN CONTABLE	Reportes de producción, ventas, inventarios, costos y contabilidad	Servidor de base de datos SQL	Equipo servidor HP ML 350 G6, asignado para la ejecución de base de datos SQL	FÍSICO
3	COMUNICACIÓN ELECTRÓNICA CON CLIENTES Y PROVEEDORES, COMUNICACIÓN INTERNA Y ALMACENAMIENTO DE INFORMACIÓN	Planificación de la calidad	Servidor de correo electrónico	Equipo servidor HP ML 310 G8, dedicado a aplicación de envío, recepción y almacenamiento de correos corporativos	FÍSICO
4	CONTRATACIÓN, HOJA DE VIDA Y LIQUIDACIÓN DE NOMINA	Proceso de contratación, hoja de vida y liquidación de nómina	Servidor de programa de nómina - SARA	Equipo servidor HP Proliant ML 310 G9 - dedicado a la aplicación de nómina SARA	FÍSICO
5	FUNCIONALIDAD PLANTA TELEFÓNICA, Y CONTROL DE LLAMADAS LD Y LDI, CELULAR, PBX	Proceso de comunicación interna y externa vía telefónica	Servidor de comunicaciones Asterix - PBX	Equipo servidor IBM - dedicado a aplicación Asterix - troncales SIP, PBX	FÍSICO
6	CONTROL, RESGUARDO Y ALMACENAMIENTO DE DOCUMENTOS DE USUARIO	Proceso de almacenamiento y protección de documentos de usuarios de la compañía	Servidor de archivos	Equipo servidor HP - ML 350 G5, dedicado al almacenamiento de documentos de usuarios de la red	FÍSICO
7	CONSOLIDAR VENTAS, INVENTARIOS Y REPORTES DE ALMACENES	Proceso de reporte por interfaz a sistema ERP	Servidor réplica AZURE, SQL, base de datos de ventas y facturación tiendas.	Servidor virtual SQL para almacenamiento de base de datos	LÓGICO
8	PROCESAMIENTO, REPORTEADOR Y ALMACENAMIENTO DE INFORMACIÓN	Procesamiento y almacenamiento de base de nómina	Base de datos de nómina	Base de datos en SQL server	LÓGICO

Cuadro 2. (Continuación)

Consecutivo	Proceso	Procedimiento	Activo	Descripción	Formato
9	PROCESAMIENTO, REPORTEADOR Y ALMACENAMIENTO DE INFORMACIÓN	Procesamiento y almacenamiento de base de nómina	Base de datos de ERP contable, costos, inventarios y producción	Base de datos en SQL server	LÓGICO
10	CAPTURA Y PROCESAMIENTO DE INFORMACIÓN	Captura y procesamiento de información contable, inventarios, costos y producción	Programa ERP PRIORITY V15	Programa ERP corporativo (contabilidad, inventarios, producción, costos y compras)	LÓGICO
11	CAPTURA Y PROCESAMIENTO DE INFORMACIÓN	Captura y procesamiento de información de nómina empleados, y hoja de vida	Programa de nómina SARA - WEB	Programa de manejo de nómina (hoja de vida, salarios, pagos, liquidaciones y pagos legales)	LÓGICO

Fuente. Elaborado por los autores.

3.1.4 Valoración. Cada activo de información fue clasificado en términos de su confidencialidad, integridad y disponibilidad, lo cual se muestra en el Cuadro 3. Calificación de la confidencialidad, Cuadro 4. Calificación de la integridad, y Cuadro 5. Calificación de la disponibilidad.

Para realizar la evaluación de cada activo se evaluó realizando una serie de preguntas específicas para determinar su nivel de impacto asignando valor de 0 a 3, en donde cero (0) no tiene impacto y tres (3) tienen impacto alto. Al finalizar se realiza un promedio de cada uno de los resultados para obtener la calificación de alto, medio y bajo, teniendo en cuenta las calificaciones obtenidas entre confidencialidad, integridad y disponibilidad, para lo cual se definieron para los rangos inferiores o iguales a 1.5 como bajo, entre 1.6 y 2.5 como medio y superiores a 2.5 como Alto.

3.1.4.1 Confidencialidad. Indica el nivel de protección que se debe aplicar a un activo de información (definido por la compañía), para evitar que su información sea comunicada o divulgada de forma indebida. Esto se muestra en el Cuadro 3. Calificación de la confidencialidad.

Cuadro 3. Calificación de la confidencialidad

Calificación de la confidencialidad					
Descripción	**¿La revelación o acceso no autorizado supondría problemas legales?**	**¿La revelación o acceso no autorizado comprometería la ejecución del proceso al cual pertenece el activo?**	**¿La revelación o acceso no autorizado causaría pérdidas económicas?**	**¿La revelación o acceso no autorizado causaría daño en reputación?**	**Promedio**
Equipo servidor HP ML 35NA G6, asignado para la ejecución de programa ERP – Priority	1	2	3	3	2.25
Equipo servidor HP ML 35NA G6, asignado para la ejecución de base de datos SQL	2	2	3	3	2.50
Equipo servidor HP ML 31NA G8, dedicado a aplicación de envío y recepción y almacenamiento de correos corporativos	2	2	3	3	2.50
Equipo servidor HP Proliant ML 31NA G9 - dedicado a la aplicación de nómina SARA	3	2	2	3	2.50
Equipo servidor IBM - dedicado a aplicación Asterix - Troncales SIP y PBX	2	2	3	3	2.50
Equipo servidor HP - ML 35NA G5, dedicado al almacenamiento de documentos de usuarios de la red	3	2	3	2	2.50

Fuente. Elaborado por los autores.

3.1.4.2 Integridad y disponibilidad. Determina el grado en el cual MODANOVA S.A.S. depende de un activo para mantener la operación y la prestación de los servicios. El activo de información clasificado como crítico es vital para la ejecución de los procesos de la empresa, ya sea porque debe ser íntegro, y/o sólo puede ser accedido por personas autorizadas y/o debe estar disponible cuando sea requerido, cuya calificación se muestra en el Cuadro 4. Calificación de la integridad, y Cuadro 5. Calificación de la disponibilidad, para cada uno de los activos.

Cuadro 4. Calificación de la integridad

Calificación de la integridad					
Descripción	**¿La alteración o modificación no autorizada del activo supondría problemas legales?**	**¿La alteración o modificación no autorizada del activo causaría toma de decisiones erradas?**	**La alteración o modificación no autorizada del activo causaría pérdidas económicas**	**¿La alteración o modificación no autorizada comprometería el(los) proceso(s)del activo, otros procesos o toda la organización?**	**Promedio**
Equipo servidor HP ML 35NA G6, asignado para la ejecución de programa ERP - Priority	2	3	3	3	2.75
Equipo servidor HP ML 35NA G6, asignado para la ejecución de base de datos SQL	2	2	2	3	2.25
Equipo servidor HP ML 31NA G8, dedicado a aplicación de envío y recepción, almacenamiento de correos corporativos	2	3	3	3	2.75
Equipo servidor HP Proliant ML 31NA G9 - dedicado a la aplicación de nómina SARA	3	3	2	3	2.75
Equipo servidor IBM - dedicado a aplicación Asterix - Troncales SIP, PBX	2	2	2	3	2.25
Equipo servidor HP - ML 35NA G5, dedicado al almacenamiento de documentos de usuarios de la red	3	3	3	3	3.00

Fuente. Elaborado por los autores.

Cuadro 5. Calificación de la disponibilidad

Calificación de la disponibilidad					
Descripción	**¿El RTO (Recovery Time Objective) es inferior a 8 horas?**	**¿La no disponibilidad del activo supondría problemas legales?**	**¿La no disponibilidad del activo causaría pérdidas económicas?**	**¿La no disponibilidad del activo comprometería la ejecución del proceso?**	**Promedio**
Equipo servidor HP ML 35NA G6, asignado para la ejecución de programa ERP - Priority	3	1	3	3	2.50
Equipo servidor HP ML 35NA G6, asignado para la ejecución de base de datos SQL	3	2	3	3	2.75
Equipo servidor HP ML 31NA G8, dedicado a aplicación de envío y recepción, almacenamiento de correos corporativos	3	2	3	3	2.75
Equipo servidor HP Proliant ML 31NA G9 - dedicado a la aplicación de nómina SARA	3	3	3	3	3.00
Equipo servidor IBM - dedicado a aplicación Asterix - Troncales SIP, PBX	3	2	3	3	2.75
Equipo servidor HP - ML 35NA G5, dedicado al almacenamiento de documentos de usuarios de la red	3	1	2	3	2.25

Fuente. Elaborado por los autores.

Al finalizar se realiza el promedio general para obtener una calificación de cada uno de los activos, cuya calificación se muestra en el Cuadro 6. Nivel de criticidad del activo.

Cuadro 6. Nivel de criticidad del activo

Consecutivo	Activo	Proceso	Procedimiento	Promedio de calificación de integridad, confidencialidad y disponibilidad	Nivel de criticidad del activo
1	Servidor de aplicación ERP	CONTABILIDAD GENERAL, FACTURACIÓN, CARTERA, INVENTARIOS, COSTOS, PRODUCCIÓN	Control de contabilidad, planeación, inventarios, costos, producción	2,50	Alto
2	Servidor de base de datos SQL	CONSOLIDACIÓN Y ALMACENAMIENTO DE INFORMACIÓN CONTABLE	Reportes de producción, ventas, inventarios, costos, contabilidad	2,50	Alto
3	Servidor de correo electrónico	COMUNICACIÓN ELECTRÓNICA CON CLIENTES Y PROVEEDORES, COMUNICACIÓN INTERNA Y ALMACENAMIENTO DE INFORMACIÓN	Planificación de la calidad	2,67	Alto
4	Servidor de programa de nómina - SARA	CONTRATACIÓN, HOJA DE VIDA, LIQUIDACIÓN DE NOMINA	Proceso de contratación, hoja de vida y liquidación de nómina	2,75	Alto
5	Servidor de comunicaciones Asterix - PBX	FUNCIONALIDAD PLANTA TELEFÓNICA Y CONTROL DE LLAMADAS LD Y LDI, CELULAR, PBX	Proceso de comunicación interna y externa, vía telefónica	2,50	Alto
6	Servidor de archivos	CONTROL, RESGUARDO Y ALMACENAMIENTO DE DOCUMENTOS DE USUARIO	Proceso de almacenamiento y protección de documentos de usuarios de la compañía	2,58	Alto

Fuente. Elaborado por los autores.

3.1.5 Matriz de Inventario y valoración de activos. Una vez determinados los activos, estos se registran en el formato de inventario haciendo referencia a aquellas características del activo que lo definen de manera única e incluye:

Consecutivo: Número consecutivo que identifica al activo en el inventario.

Activo: Nombre de identificación del activo dentro del proceso al que pertenece.

Tipo de activo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

- **Activo físico**, Categoría: **Tecnología**: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PC, teléfonos, impresoras, routers, cableado, etc.)

- **Activo software**, Categoría: **Aplicaciones**: El software que se utiliza para la gestión de la información.

- **Activo información**, Categoría: **Datos**: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

Descripción: Es un espacio para describir el activo de manera que sea claramente identificable por todos los interesados.

Formato: Físico o Lógico.

Procesos: Procesos en los que participa el activo.

Criticidad: Es la criticidad que toma el activo luego de hacer el inventario y valorarlo.

El resultado de este proceso se muestra en el Cuadro 7. Activos críticos de MODANOVA S.A.S.

Cuadro 7. Activos críticos de modanova

Consecutivo	Activo	Tipo de activo	Descripción	Formato	Procesos	Criticidad
1	Servidor de aplicación ERP	Activo Físico (Tecnología)	Equipo Servidor HP ML 35NA G6, asignado para la ejecución de programa ERP - Priority	FÍSICO	CONTABILIDAD GENERAL, FACTURACIÓN, CARTERA, INVENTARIOS, COSTOS, PRODUCCIÓN	Activo de información Crítico

Cuadro 7. (Continuación)

Consecutivo	Activo	Tipo de activo	Descripción	Formato	Procesos	Criticidad
2	Servidor de base de datos SQL	Activo Físico (Tecnología)	Equipo Servidor HP ML 35NA G6, asignado para la ejecución de base de datos SQL	FÍSICO	CONSOLIDACIÓN Y ALMACENAMIENTO DE INFORMACIÓN CONTABLE	Activo de información Crítico
3	Servidor de correo electrónico	Activo Físico (Tecnología)	Equipo Servidor HP ML 31NA G8, dedicado a aplicación de envío y recepción, almacenamiento de correos corporativos	FÍSICO	COMUNICACIÓN ELECTRÓNICA CON CLIENTES Y PROVEEDORES, COMUNICACIÓN INTERNA Y ALMACENAMIENTO DE INFORMACIÓN	Activo de información Crítico
4	Servidor de programa de nómina - SARA	Activo Físico (Tecnología)	Equipo Servidor HP Proliant ML 31NA G9 - dedicado a la aplicación de Nomina Sara	FÍSICO	CONTRATACIÓN, HOJA DE VIDA, LIQUIDACIÓN DE NOMINA	Activo de información Crítico
5	Servidor de comunicaciones Asterix - PBX	Activo Físico (Tecnología)	Equipo Servidor IBM - dedicado a aplicación Asterix - Troncales SIP, PBX	FÍSICO	FUNCIONALIDAD PLANTA TELEFÓNICA Y CONTROL DE LLAMADAS LD Y LDI, CELULAR, PBX	Activo de información Crítico
6	Servidor de archivos	Activo Físico (Tecnología)	Equipo Servidor HP - ML 35NA G5, dedicado al almacenamiento de documentos de usuarios de la RED	FÍSICO	CONTROL, RESGUARDO Y ALMACENAMIENTO DE DOCUMENTOS DE USUARIO	Activo de información Crítico
7	Servidor Replica AZURE, SQL, Base De Datos De Ventas y facturación tiendas.	Activo Lógico (Tecnología)	Servidor Virtual SQL para almacenamiento de base de datos de	LÓGICO	CONSOLIDAR VENTAS, INVENTARIOS, REPORTES DE ALMACENES	Activo de información Crítico

Fuente. Elaborado por los autores.

3.1.6 Actualización. La actividad de actualización se refiere a la verificación que se lleva a cabo para determinar si un activo continúa o no siendo parte del inventario, o si deben incluirse nuevos activos.

3.2 CRITERIOS DE VALORACIÓN DE RIESGOS

3.2.1 Niveles de riesgo. Se consideraron 4 niveles de riesgo los cuales se derivan de la combinación directa del nivel de probabilidad y del impacto evaluado. Estos valores se organizan en una matriz denominada mapa de riesgo y permite la visualización rápida de los riesgos identificados por cada activo de información.

3.2.1.1 Definición de los niveles de riesgo. Los niveles de riesgo son utilizados para asignar en una escala definida de que tan importante o prioritario es un riesgo, de esta forma al momento de decidir podrá seleccionarse en base a prioridades.

Para este proyecto se crea un cuadro de niveles de riesgo basado en 4 tipos de criticidades.

Para la realización de este análisis se definieron los niveles de riesgo que se muestran en el Cuadro 8. Definición de niveles de riesgo.

Cuadro 8. Definición de niveles de riesgo

Niveles de riesgo	Definición
Extremo	Corresponde a los riesgos críticos con alta probabilidad de ocurrencia y un impacto grave, en caso de su materialización. Se debe priorizar la toma de acciones de mitigación lo más pronto posible para proteger y garantizar la seguridad del activo.
Alto	Probabilidad media de ocurrencia e impacto alto, requiere tiempos efectivos de aplicación de remediación.
Moderado	Requieren acciones correctivas y de mitigación a desarrollar en un periodo razonable de tiempo.
Bajo	Corresponde a los riesgos no significativos o de poco impacto y no son necesarios planes correctivos o de mitigación.

Fuente. Elaborado por los autores.

La evaluación del nivel de probabilidad de que una vulnerabilidad sea aprovechada por una amenaza potencial se debe determinar de acuerdo con el Cuadro 9. Niveles de probabilidad.

El Cuadro 9. Niveles de probabilidad, se definió en cuanto a facilidad de explotación y nivel de exposición de la vulnerabilidad debido a que MODANOVA S.A.S. carece de área de seguridad informática, estadísticas de ataques y vulnerabilidades identificadas. No hay cifras estadísticas para establecer porcentajes de probabilidad cuantificables de ataques y por ello se elabora el Cuadro 9. Niveles de probabilidad, basado en la facilidad de explotación de vulnerabilidades a nivel cualitativo.

Cuadro 9. Niveles de probabilidad

Nivel de probabilidad	Definición
Muy alta	Se espera que ocurra en un periodo no mayor a 6 meses. Fácilmente explotable.
Alta	Se espera que ocurra en un periodo no mayor a 8 meses. Existe una alta motivación de aprovechar la vulnerabilidad y los controles existentes son inefectivos para evitar que se aproveche.

Cuadro 9. (Continuación)

Nivel de probabilidad	Definición
Moderada	Se espera que ocurra en un periodo no mayor a 12 meses. Hay motivación de aprovechar la vulnerabilidad, pero los controles existentes pueden evitar que se aproveche.
Baja	Se espera que, de explotarse, esto suceda en un periodo mayor a 12 meses. No hay una motivación conocida para aprovechar la vulnerabilidad y además existen controles para evitar que se aproveche.

Fuente. Elaborado por los autores.

La evaluación del nivel de impacto negativo, resultado de la materialización de una amenaza sobre una vulnerabilidad se debe determinar con los valores que se presentan en el Cuadro 10. Niveles de impacto, se deben considerar como impacto negativo la perdida directa de dinero, responsabilidad penal o civil, pérdida de reputación, conflictos con clientes, violaciones a la confidencialidad de la información de clientes o de la organización, pérdida de oportunidades, pérdida de participación, reducción en el desempeño operativo, interrupción en la prestación de los servicios o violación a leyes y regulaciones que generen sanciones.

Para la realización de este análisis en MODANOVA S.A.S. se definieron los niveles de impacto a utilizar en la elaboración de este proyecto, los cuales se muestran en el Cuadro 10. Niveles de impacto.

Cuadro 10. Niveles de impacto

Nivel de impacto	Definición
Superior	Interrupción total de la prestación de los servicios, pérdida de información no recuperable o revelación de información confidencial de clientes o de la organización que genere multas, pérdida de oportunidad, responsabilidad penal o civil, o violación a leyes y regulaciones.
Mayor	Interrupción parcial de la prestación de los servicios, pérdida de la capacidad de operación, violaciones a la política de seguridad de la organización que generan pérdidas financieras importantes.
Importante	Interrupción en la prestación de los servicios debidas a la alteración, revelación o indisponibilidad de activos de información y que generen perdida de reputación, conflictos con clientes, pérdida de participación o reducción del desempeño operativo.
Menor	Alteración o pérdida de activos de información que generan reducción en el desempeño o interrupciones menores en la prestación del servicio y que no generan sanciones ni multas de ningún tipo.

Fuente. Elaborado por los autores.

Para la elaboración de este análisis de vulnerabilidades en MODANOVA S.A.S, se definió el mapa de riesgo que se muestra en el Cuadro 11. Mapa de riesgo (Probabilidad x Impacto).

Cuadro 11. Mapa de riesgo (probabilidad x Impacto)

Combinaciones de riesgo	**Impacto**				
Probabilidad	Inferior	Menor	Importante	Mayor	Superior
Muy alta	Bajo	Moderado	Alto	Extremo	Extremo
Alta	Bajo	Moderado	Alto	Alto	Extremo
Moderada	Bajo	Moderado	Moderado	Alto	Alto
Baja	Bajo	Bajo	Moderado	Moderado	Moderado
Muy baja	Bajo	Bajo	Bajo	Bajo	Bajo

Fuente. Elaborado por los autores.

3.2.1.2 Aceptación del riesgo. El Cuadro 12. Niveles de riesgo aceptables, se elaboró para registrar los niveles de aceptabilidad de los riesgos encontrados en MODANOVA S.AS.

Cuadro 12. Niveles de riesgo aceptables

Niveles de riesgo	**Aceptabilidad**
Extremo	No Aceptable por sus niveles de probabilidad de ocurrencia e impacto debe dársele tratamiento.
Alto	No Aceptable por sus niveles de probabilidad de ocurrencia e impacto debe dársele tratamiento.
Moderado	No Aceptable por sus niveles de probabilidad de ocurrencia e impacto debe dársele tratamiento.
Bajo	Aceptable.

Fuente. Elaborado por los autores.

3.3 IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Durante el levantamiento de la información que se realizó en MODANOVA S.A.S. se identificaron los siguientes procesos que se muestran en el Cuadro 13. Procesos críticos. Estos son los procesos críticos de generación, proceso y almacenamiento de información.

Cuadro 13. Procesos críticos

Proceso	**Descripción**
Venta POS	Información de ventas de todos los almacenes.
Contabilidad	Ingreso y procesamiento de información contable.

Cuadro 13. (Continuación)

Proceso	Descripción
Facturación	Proceso de venta mayorista.
Inventarios	Proceso de control de inventarios.
Costos	Proceso de cálculo de rentabilidad.
Producción	Proceso de fabricación de productos.
Planeación	Proceso de programación y proyección de fabricación.
Nómina	Proceso de cálculo de nómina y pagos de empleados.

Fuente. Elaborado por los autores.

3.4 INVENTARIO DE SOFTWARE

Dentro del levantamiento de información que se realizó en MODANOVA S.A.S. se identificó el software instalado en los activos críticos que involucran manejo de información crítica, esto se documentó en el Cuadro 14. Inventario de software.

Cuadro 14. Inventario de software

Tipo	Descripción	Versión
Sistema operativo	Microsoft Windows Server Std	2008 R2
Sistema operativo	Microsoft Windows Server Std	2008
Sistema operativo	Linux CentOS	6
Sistema operativo	Linux CentOS	5
Programa	Microsoft SQL Server	2008
Programa	Microsoft Office Std	2007
Programa	Priority ERP	15
Programa	Nómina SARA	10
Programa	Asterisk PBX	11
Programa	Antivirus Kaspersky	10

Fuente. Elaborado por los autores.

3.5 IDENTIFICACIÓN DE VULNERABILIDADES

De acuerdo con el enfoque metodológico de gestión de riesgo, se tomaron los activos de T.I. clasificados como críticos en el inventario y se identificaron las vulnerabilidades que tienen estos activos en su tratamiento, almacenamiento o configuración y que pueden ser explotadas por las amenazas para causar daños a los activos, pérdida de información o fugas de la misma.

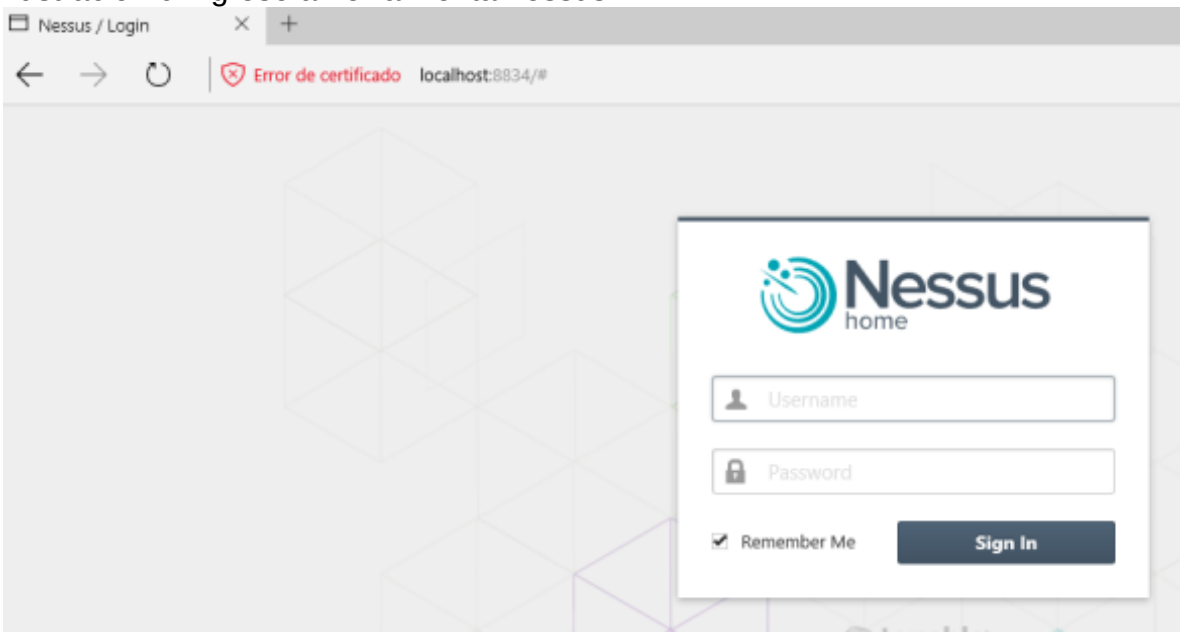
Para la elaboración del análisis de vulnerabilidades en MODANOVA S.A.S., se utilizó la herramienta Nessus en la versión 6.8.1 para Windows como se evidencia en la Ilustración 5. Descarga de versión de nessus.

Ilustración 5. Descarga de versión de nessus

Fuente. Elaborada por los autores.

Ya instalado se ejecuta como se aprecia en la Ilustración 6. Ingreso a herramienta nessus.

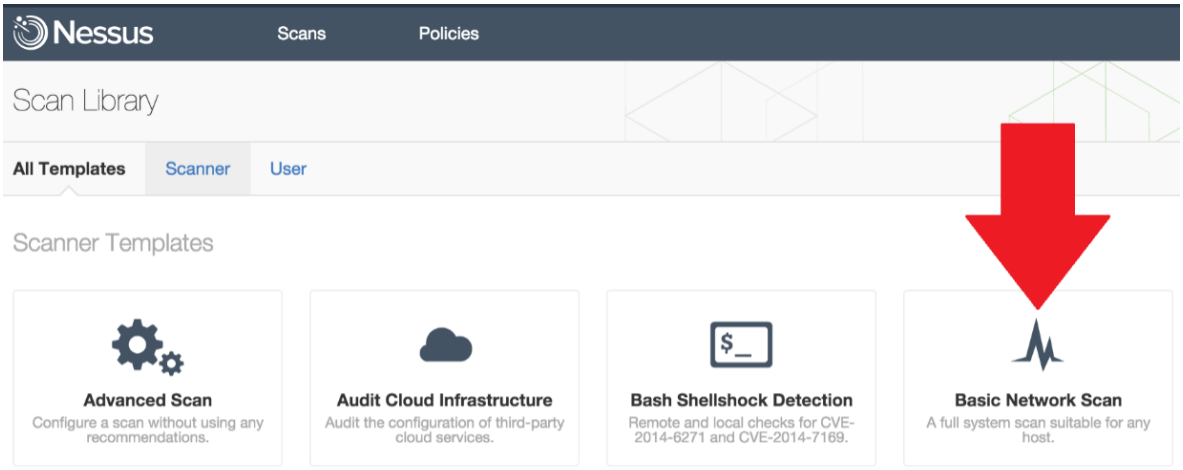
Ilustración 6.Ingreso a herramienta nessus



Fuente. Elaborada por los autores.

En la Ilustración 7. Análisis de Nessus, se aprecia que se realiza un escaneo competo con la opción Basic Network Scan, en donde se configuraron cada una de las direcciones IP de los activos críticos para su respectivo análisis.

Ilustración 7.Análisis de nessus



Fuente. Elaborada por los autores.

Una vez realizado los análisis la herramienta entrega los resultados y sus hallazgos para cada uno de los activos como se observa en la muestra de la Ilustración 8. Resultados del análisis de Nessus y en la Ilustración 9. Reporte resumen de vulnerabilidades.

Ilustración 8.Resultados del análisis de nessus

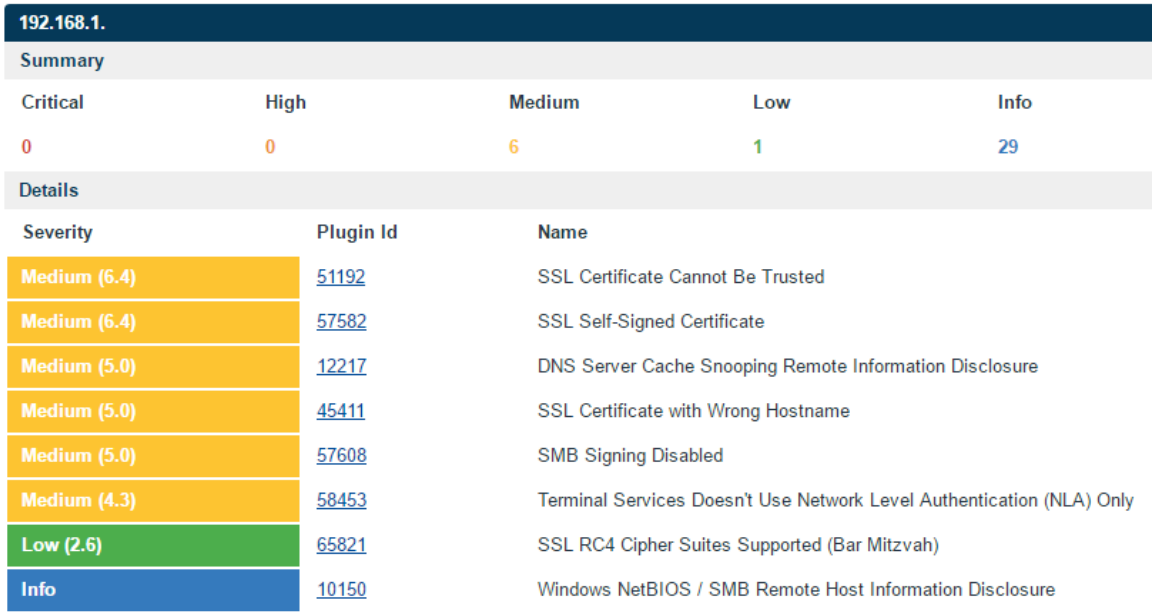
192.168.1. XXX

Scan Information	
Start time:	Tue Jul 12 20:21:30 2016
End time:	Tue Jul 12 20:29:39 2016
Host Information	
DNS Name:	xxxx.modanova.com.co
Netbios Name:	SERV-TERM
IP:	192.168.1. xxx
MAC Address:	00:15:5d: xx:xx:xx
OS:	Microsoft Windows Server 2008 Standard Service Pack 2

Results Summary			
Critical	High	Medium	Low
0	0	6	1

Fuente. Elaborada por los autores.

Ilustración 9.Reporte resumen de vulnerabilidades



192.168.1.

Summary

Critical	High	Medium	Low	Info
0	0	6	1	29

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

Fuente. Elaborada por los autores.

Una vez terminado el análisis en cada uno de los activos de MODANOVA S.A.S. se encontraron un total **63** vulnerabilidades respecto a los activos críticos de T.I., como se muestra en el Cuadro 15. Resumen de vulnerabilidades encontradas.

Cuadro 15. Resumen de vulnerabilidades encontradas

Activo de T.I.	Nivel de vulnerabilidades	Cantidades	Total
Servidor de aplicación ERP	Crítico	0	7
	Alto	0	
	Medio	6	
	Bajo	1	
Servidor de base de datos SQL	Crítico	3	24
	Alto	6	
	Medio	12	
	Bajo	3	
Servidor de programa nómina - SARA	Crítico	0	6
	Alto	0	
	Medio	5	
	Bajo	1	
Servidor de comunicaciones Asterix - PBX	Crítico	0	14
	Alto	0	
	Medio	11	
	Bajo	3	

Cuadro15. (Continuación)

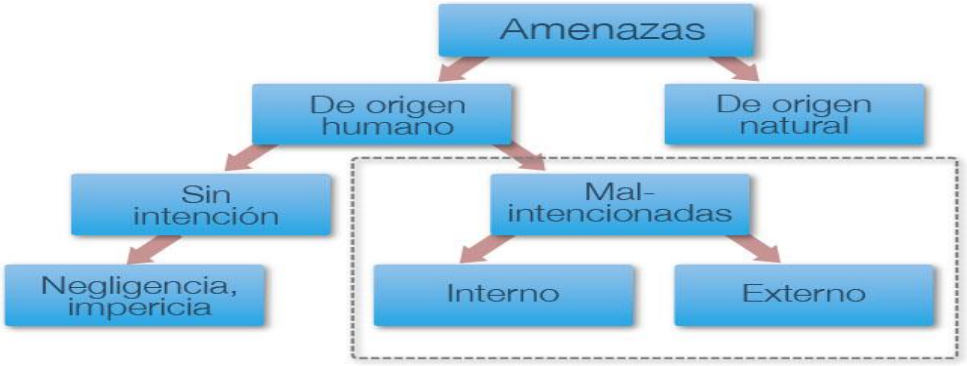
Activo de T.I.	Nivel de vulnerabilidades	Cantidades	Total
Servidor de correo electrónico	Crítico	0	8
	Alto	0	
	Medio	3	
	Bajo	5	
Servidor de archivos	Crítico	0	4
	Alto	0	
	Medio	3	
	Bajo	1	

Fuente. Elaborado por los autores.

3.6 IDENTIFICACIÓN DE AMENAZAS

Una amenaza tiene el potencial de causar daños a los activos al explotar las vulnerabilidades, estas pueden ser de origen humano o de origen natural, la clasificación completa se evidencia en el Gráfico 4. Clasificación de amenazas.

Gráfico 4. Clasificación de amenazas



Fuente. Elaborado por los autores.

Una vez identificadas las vulnerabilidades de los Activos críticos de T.I. de MODANOVA S.A.S., se procedió a encontrar las amenazas potenciales que podrían aprovechar estas vulnerabilidades, tomando como base el catálogo de amenazas de la NTC-ISO/IEC 27005 Anexo C, el cual se muestra en el Cuadro 16. Tipos de amenazas.

Cuadro 16. Tipos de amenazas

Tipo	Amenazas
Mal intencionadas (De origen Humano)	Acceso físico no autorizado a las instalaciones.
	Atacante explota vulnerabilidades en sistemas y/o aplicaciones.
	Acceso no autorizado al sistema.
	Atacante realiza denegación de servicio distribuido (DDoS).
	Atacante compromete la infraestructura de un proveedor.
	Atacante Realiza ataque utilizando puertos, protocolos y servicios no autorizados.
	Atacante recopila información pública para efectuar un ataque.
	Atacante identifica componentes, recursos u obtiene información haciendo sniffing sobre la red.
	Difusión de software malicioso.
	Atacante accede a sistemas de información expuestos en internet.
	Atacante compromete equipo de usuario con privilegios de conexión remota.
	Abuso de privilegios de acceso.
	Ingeniería Social.
	Interceptación de tráfico de información sensible.
	Extorsión.
	Fuga de información.
	Robo de información.
	Suplantación de identidad de usuario.
	Robo de hardware.
	Descarga de software no autorizada.
Ambiental (De origen Natural)	Fuego.
	Inundación.
	Temblor.
Falla Técnica	Falla de suministro de energía.
	Falla de suministro de energía de respaldo.
	Subidas de voltaje fluctuaciones.
	Carga eléctrica.
	Falla/degradación de equipo informático.
	Falla/degradación de sistemas de comunicaciones.
	Falla de aire acondicionado.
	Saturación del Sistema de información.
	Corrupción de datos.
	Negación de servicio.
No deliberadas	Inadvertida exposición de información crítica.
	Error de Usuario.
	Error de Administrador.
	Error de Configuración.
	Uso no previsto.
	Destrucción de información.
	Perdida de hardware.
	Indisponibilidad del personal.

Fuente. Elaborado por los autores.

3.7 IDENTIFICACIÓN DE RIESGOS

Durante el proceso de identificación de riesgos sobre los activos críticos de T.I., se identificaron 8 riesgos de seguridad de la información. Los riesgos identificados se listan y describen en el Cuadro 17. Riesgos identificados.

Cuadro 17. Riesgos identificados

Consecutivo	Activos	Riesgo	Descripción del riesgo
1	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Los certificados autofirmados generan alertas que dan lugar a advertencias en el navegador. Los empleados podrían acostumbrarse a ignorar estar alertas generadas por el navegador también en la navegación en sitios públicos, exponiéndose a descargar malware y otras amenazas. Dado que un certificado autofirmado no es "manejado" por una autoridad certificadora, no hay revocación (anular su validez del certificado) en caso de que un atacante robe la clave privada.
2	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Al tener una cantidad tan alta de vulnerabilidades críticas en la infraestructura se demuestra que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la empresa a un ataque.
3	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de confidencialidad.	Un atacante puede hacer un ataque de hombre en el medio explotando la vulnerabilidad de POODLE al permitirse SSL v3.0.
4	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de integridad.	Configuraciones y credenciales por defecto en las aplicaciones podrían permitir la modificación, eliminación o visualización contenida en las bases de datos.
5	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de confidencialidad, integridad y disponibilidad.	El contar con vulnerabilidades que datan de hace 8 años o más, demuestran que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la empresa a un ataque.
6	SERVIDOR DE COMUNICACIONES ASTERIX - PBX.	Pérdida de confidencialidad.	Un atacante puede ejecutar un ataque de hombre en el medio aprovechando las múltiples fallas del protocolo criptográfico.
7	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Al comprometer una máquina de usuario, un atacante podría ver todos los servidores, enumerar todos los servicios de cada uno de ellos y explotar aquellos servicios que sean vulnerables.
8	SERVIDOR DE APLICACIÓN ERP.	Pérdida de disponibilidad.	Cambios a nivel de sistema operativo o de aplicación implementados directamente en ambiente de producción podrían generar indisponibilidad del Sistema de información.

Fuente. Elaborado por los autores.

3.8 EVALUACIÓN DE RIESGOS

Se establecieron los niveles de riesgo de acuerdo a la combinación de probabilidad por impacto, como lo establece el mapa de calor del Cuadro 18. Combinaciones de riesgo. Donde rojo es extremo, amarillo es alto, azul es moderado y verde es bajo.

Cuadro 18. Combinaciones de riesgo

Combinaciones de riesgo	**Impacto**				
Probabilidad	Inferior	Menor	Importante	Mayor	Superior
Muy alta	Bajo	Moderado	Alto	Extremo	Extremo
Alta	Bajo	Moderado	Alto	Alto	Extremo
Moderada	Bajo	Moderado	Moderado	Alto	Alto
Baja	Bajo	Bajo	Moderado	Moderado	Moderado
Muy baja	Bajo	Bajo	Bajo	Bajo	Bajo

Fuente. Elaborado por los autores.

Se diligenció el Cuadro 19. Evaluación de riesgos, identificando vulnerabilidades, amenazas, impactos y probabilidades. El nivel de riesgo es calculado de acuerdo a las combinaciones de riesgos (probabilidad por impacto).

Cuadro 19. Evaluación de riesgos

Consecutivo	Riesgo	Vulnerabilidad	Amenaza	Impacto	Probabilidad	Nivel de riesgo
1	Pérdida de confidencialidad de la información	Certificado digital autofirmados	Interceptación de tráfico de información sensible	Importante	Moderada	Moderado
2	Pérdida de confidencialidad de la información	Número elevado de vulnerabilidades de nivel crítico y medio encontradas en los activos críticos de T.I.	Atacante explota Vulnerabilidades en sistemas y/o aplicaciones	Superior	Muy alta	Extremo
3	Pérdida de confidencialidad de la información	Uso de protocolos criptográficos obsoletos e inseguros (SSL v 3.0)	interceptación de tráfico de información sensible	Mayor	Alta	Alto
4	Pérdida de Integridad de la información.	Software con debilidad en la configuración (configuraciones por defecto inseguras)	Acceso no autorizado al sistema	Mayor	Muy alta	Extremo

Cuadro 19. (Continuación)

Consecutivo	Riesgo	Vulnerabilidad	Amenaza	Impacto	Probabilidad	Nivel de riesgo
5	Pérdida de Integridad de la información.	El sistema registra vulnerabilidad critica de 2007	interceptación de tráfico de información sensible	Mayor	Alta	Alto
6	Pérdida de confidencialidad de la información	Uso de protocolos criptográficos obsoletos e inseguros (SSL v 2.0)	interceptación de tráfico de información sensible	Mayor	Muy alta	Extremo
7	Pérdida de confidencialidad de la información	Al estar los servidores en el mismo segmento de red de los equipos de usuario. No existe filtro e independencia de tráfico para los servidores	Atacante realiza ataque utilizando puertos, protocolos y servicios no autorizados.	Superior	Moderada	Alto
8	Pérdida de disponibilidad de la información	No existe ambiente de pruebas	Error de configuración	Superior	Moderada	Alto

Fuente. Elaborado por los autores.

Utilizando como base, el Cuadro 18. Combinaciones de riesgo, se suprimen los textos bajo, moderado, alto y extremos y se ubican en sus casillas la cantidad correspondiente de riesgos de acuerdo a los impactos y probabilidades del Cuadro 19. Evaluación de riesgos; de este modo se genera el Cuadro 20. combinaciones de riesgo identificados, el cual es la presentación de los riesgos en un mapa de calor.

Cuadro 20. Combinaciones de riesgo identificados

Combinaciones de riesgo	**Impacto**				
Probabilidad	Inferior	Menor	Importante	Mayor	Superior
Muy alta				2	1
Alta				2	
Moderada			1		2
Baja					
Muy baja					

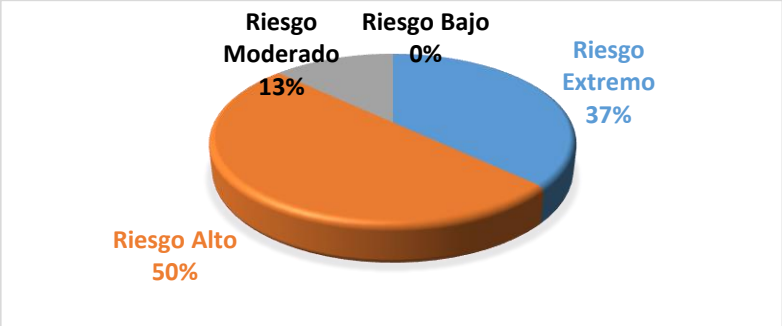
Fuente. Elaborado por los autores.

De los 8 riesgos identificados, todos se encuentran en niveles no aceptables (R1, R2, R3, R4, R5, R6, R7, R8) como se definió en la sección 3.2.1.2 Aceptación del riesgo, por lo tanto, deben ser remediados con la implementación de controles y

ningún riesgo se ubica en niveles aceptables, de acuerdo con los criterios de aceptación de riesgos definidos.

El 50% de los riesgos se encuentran en nivel alto, el 37% en nivel extremo y el 13% en nivel moderado como lo muestra el Gráfico5. Distribución de niveles de riesgo.

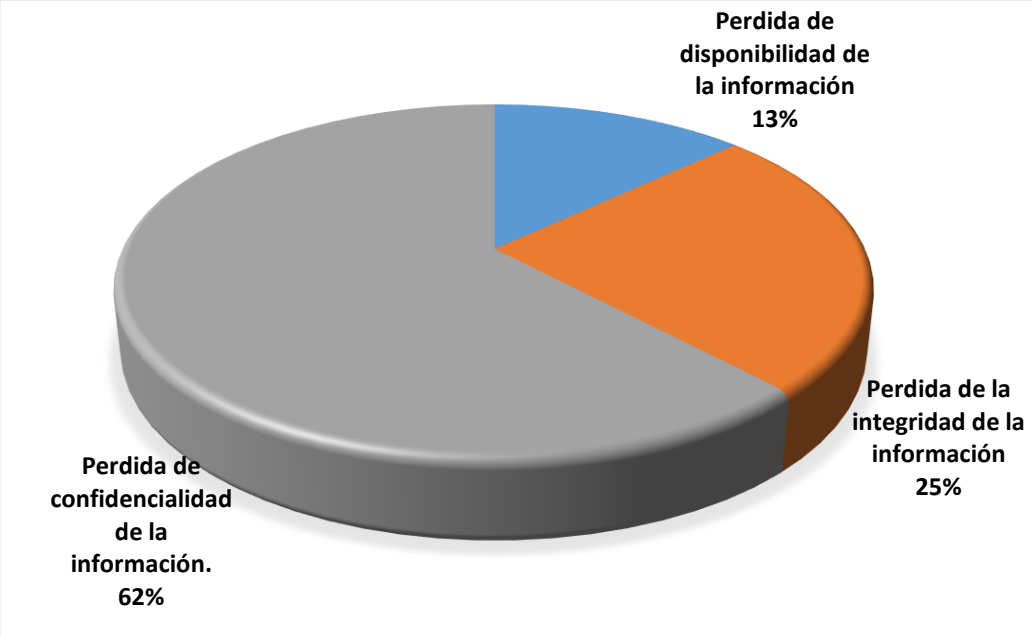
Gráfico 5. Distribución de niveles de riesgo



Fuente. Elaborado por los autores.

Los 8 riesgos de seguridad de la información se distribuyen de acuerdo al Gráfico 6. Distribución de tipos de riesgo, basados en el aspecto de seguridad involucrado.

Gráfico 6. Distribución de tipos de riesgo



Fuente. Elaborado por los autores.

3.9 TRATAMIENTO DEL RIESGO

Los planes de tratamiento de riesgo se desarrollan para los riesgos con nivel extremo y para los riesgos de nivel alto; considerados riesgos no aceptables, dejando como opcionales a decisión de la alta gerencia el tratamiento de los riesgos menores. La prioridad es la mitigación de los riesgos en nivel extremo y los riesgos de nivel bajo se consideran riesgos aceptables que no requieren el desarrollo de planes de tratamiento.

El plan de tratamiento diseñado para MODANOVA S.A.S. sugiere controles basados en la norma ISO/IEC 27002:2013 para mitigar (reducir, retener, evitar, o transferir) los riesgos informáticos identificados que se encuentran en niveles no aceptables y así reducir sus niveles de impacto o probabilidad de ocurrencia.

El plan de trabajo para la implementación de los controles se basa en los controles citados en el Cuadro 21. Controles sugeridos, y básicamente es implementar 10 controles:

- Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
- Desarrollar estándares de configuración de aseguramiento para sistemas operativos, bases de datos, dispositivos de red y aplicaciones.
- Cambiar configuraciones por defecto.
- Desarrollo de la política de controles criptográficos.
- Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior.
- Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.
- Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).
- Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción.
- Implementación de entidad certificadora de confianza.
- Cambiar certificados auto firmados por certificados de confianza.

Cuadro 21. Controles sugeridos

Consecutivo	Controles sugeridos ISO 27002	Actividades de control
1	A. 10.1.1 Política sobre el uso de controles criptográficos. A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Desarrollo de la política de controles criptográficos. Implementación de entidad certificadora de confianza. Cambiar certificados autofirmados por certificados de confianza.

Cuadro 21. (Continuación)

Consecutivo	Controles sugeridos ISO 27002	Actividades de control
1	A. 10.1.1 Política sobre el uso de controles criptográficos. A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Desarrollo de la política de controles criptográficos. Implementación de entidad certificadora de confianza. Cambiar certificados autofirmados por certificados de confianza.
2	A. 12.6.1 Gestión de las vulnerabilidades técnicas.	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
3	A. 10.1.1 Política sobre el uso de controles criptográficos.	Desarrollo de la política de controles criptográficos. Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.
4	A. 14.1.1 Análisis y especificación de requisitos de seguridad de la información.	Desarrollar estándares de configuración segura para sistemas operativos, bases de datos, dispositivos de red y aplicaciones. Cambiar configuraciones por defecto.
5	A. 12.6.1 Gestión de las vulnerabilidades técnicas.	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
6	A. 10.1.1 Política sobre el uso de controles criptográficos.	Desarrollo de la política de controles criptográficos. Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior.
7	A 13.1.3 Separación en las redes.	Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).
8	A. 12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción.

Fuente. Elaborado por los autores.

4. PLAN DE TRABAJO PARA IMPLEMENTAR LOS CONTROLES

4.1 DIAGNÓSTICO DE LA SITUACIÓN

Este plan de trabajo se elabora con una serie de actividades para aplicar los controles resultantes del diseño metodológico y que puedan mitigar los riesgos de los activos críticos de T.I. de MODANOVA S.A.S.

Se identificaron 8 Riesgos de los cuales hay 3 extremos, 4 altos y 1 moderado, y se ofrece mitigación a los mismos mediante la sugerencia de 10 controles los cuales resultan ser transversales a varios riesgos; es decir, un control puede mitigar más de un riesgo y un riesgo puede requerir más de un control.

Los principales activos impactados son 6 servidores valorados como críticos para el negocio de acuerdo a los niveles requeridos de confidencialidad, integridad y disponibilidad (servidor de aplicación ERP, servidor de archivos, servidor de base de datos SQL, servidor de comunicaciones Asterix - PBX, servidor de correo electrónico y servidor de programa de nómina - Sara).

Dado que en el proyecto se identificaron y evaluaron 8 riesgos, se hace relación de los mismos en el Cuadro 22. Riesgos identificados.

Cuadro 22. Riesgos identificados

Consecutivo	Activos	Riesgo	Descripción del riesgo
1	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Los certificados autofirmados generan alertas que dan lugar a advertencias en el navegador. Los empleados podrían acostumbrarse a ignorar estar alertas generadas por el navegador también en la navegación en sitios públicos, exponiéndose a descargar malware y otras amenazas. Dado que un certificado autofirmado no es "manejado" por una CA, no hay revocación (anular su validez del certificado) en caso de que un atacante robe la clave privada.
2	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Al tener una cantidad tan alta de vulnerabilidades críticas en la infraestructura se demuestra que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la empresa a un ataque.

Cuadro 22. (Continuación)

Consecutivo	Activos	Riesgo	Descripción del riesgo
3	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de confidencialidad.	Un atacante puede hacer un ataque de hombre en el medio explotando la vulnerabilidad de POODLE al permitirse SSL v3.0.
4	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de integridad.	Configuraciones y credenciales por defecto en las aplicaciones podrían permitir la modificación, eliminación o visualización contenida en las bases de datos.
5	SERVIDOR DE BASE DE DATOS SQL.	Pérdida de confidencialidad, integridad y disponibilidad.	El Contar con vulnerabilidades que datan de hace 8 años o más, demuestran que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la empresa a un ataque.
6	SERVIDOR DE COMUNICACIONES ASTERIX - PBX.	Pérdida de confidencialidad.	Un atacante puede ejecutar un ataque de hombre en el medio aprovechando las múltiples fallas del protocolo criptográfico.
7	SERVIDOR DE APLICACIÓN ERP, SERVIDOR DE BASE DE DATOS SQL, SERVIDOR DE PROGRAMA DE NÓMINA - SARA, SERVIDOR DE COMUNICACIONES ASTERIX - PBX, SERVIDOR DE CORREO ELECTRÓNICO Y SERVIDOR DE ARCHIVOS.	Pérdida de confidencialidad.	Al comprometer una máquina de usuario, un atacante podría ver todos los servidores, enumerar todos los servicios de cada uno de ellos y explotar aquellos servicios que sean vulnerables.
8	SERVIDOR DE APLICACIÓN ERP.	Pérdida de disponibilidad.	Cambios a nivel de sistema operativo o de aplicación implementados directamente en ambiente de producción podrían generar indisponibilidad del Sistema de información.

Fuente. Elaborado por los autores.

Al igual que con la relación del detalle de los riesgos, se presenta la relación de los controles sugeridos para mitigar los riegos junto a las actividades de control, esto se puede apreciar en el Cuadro 23. Controles sugeridos.

Cuadro 23. Controles sugeridos

Consecutivo	Controles sugeridos ISO 27002	Actividades de control
1	A. 10.1.1 Política sobre el uso de controles criptográficos. A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Desarrollo de la política de controles criptográficos.
		Implementación de entidad certificadora de confianza.
		Cambiar certificados autofirmados por certificados de confianza.

Cuadro 23. (Continuación)

Consecutivo	Controles sugeridos ISO 27002	Actividades de control
2	A. 12.6.1 Gestión de las vulnerabilidades técnicas.	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
3	A. 10.1.1 Política sobre el uso de controles criptográficos.	Desarrollo de la política de controles criptográficos. Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.
4	A. 14.1.1 Análisis y especificación de requisitos de seguridad de la información.	Desarrollar Estándares de configuración segura (hardening) para sistemas operativos, bases de datos, dispositivos de red y aplicaciones. Cambiar configuraciones por defecto.
5	A. 12.6.1 Gestión de las vulnerabilidades técnicas.	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
6	A. 10.1.1 Política sobre el uso de controles criptográficos.	Desarrollo de la política de controles criptográficos. Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior.
7	A 13.1.3 Separación en las redes.	Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).
8	A. 12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.	Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción

Fuente. Elaborado por los autores.

4.2 ASIGNACIÓN DE RECURSOS

Se citan a continuación los recursos mínimos y generales que se requieren para aplicar los controles del proyecto, pero cada control puede requerir inversión de nuevo software, nuevo hardware y servicios profesionales los cuales se citan en detalle en cada control. La alta gerencia evaluará que riesgos con sus controles desea mitigar y un criterio para decidir cuales excluir es el costo de estos recursos adicionales.

4.2.1 Humanos.

- Gerente general.
- Gerente de proyecto (si se desea trabajar el plan como un proyecto).
- Jefe de sistemas.
- Líder técnico.
- Ingeniero o técnico.
- Especialista en seguridad informática o ingeniero con esta característica.

4.2.2 Técnicos/Tecnológicos. Los controles 8 y 9 requieren inversión en nuevos activos.

Control 8. Mínimo 6 Servidores con características físicas lo más similares posibles a los Activos críticos de T.I. identificados en el proyecto y licenciamiento del software presente en estos 6 servidores.

Control 9. Un servidor que soporte Windows Server 2012 con una Licencia de Windows Server 2012.

4.3 ASIGNACIÓN DE TAREAS, FUNCIONES Y RESPONSABILIDADES

4.3.1 Especialista en seguridad informática. Responsable de la ejecución, modificaciones o sugerencias frente al plan de trabajo.

4.3.2Gerente general. Aprobar plan de trabajo, aprobar los riesgos de interés a trabajar y asignar los recursos físicos, tecnológicos y humanos.

4.3.3 Jefe de sistemas. Facilitar información necesaria y recursos aprobados para el proyecto.

4.3.4 Líder técnico. Cotizar o presentar propuesta económica de la implementación de los controles sugeridos.

4.3.5 Ingeniero o técnico. Ejecutar actividades técnicas ordenadas por el líder técnico como instalación de software, aplicación de configuraciones y levantamientos de información.

4.3.6 Gerente del proyecto. Liderar el proyecto de implementación del plan de remediación de riesgos, presentar informes periódicos sobre el avance del proyecto y hacer seguimiento de las actividades aprobadas.

4.4 METODOLOGÍA

4.4.1 Enfoque del plan. Algunos de los controles a implementar inciden en más de uno de los riesgos mencionados en el proyecto, razón por la cual el plan de trabajo se basa en los controles priorizando en los que aplican sobre los riesgos del más extremo hasta el menor.

Los controles se abordarán iniciando con la criticidad del riesgo en que se encuentren, de ahí la razón por la cual previamente se reordenaron los controles para implementasen primero los que solucionen los riesgos extremos, luego altos y finalmente Moderados.

4.4.2 Cambio de terminología por abreviaturas. Para facilitar el análisis de la información, se decidió emplear abreviaturas para los riesgos y controles. De este modo los riesgos empiezan con R y los controles con C, generándose las abreviaturas citadas en el Cuadro 24. Abreviaturas de riesgos, para los riesgos y Cuadro 25. Abreviaturas de controles, para los controles.

Cuadro 24. Abreviaturas de riesgos

Riesgos	Descripción
R1	Los certificados auto firmados generan alertas que dan lugar a advertencias en el navegador. Los empleados podrían acostumbrarse a ignorar estar alertas generadas por el navegador también en la navegación en sitios públicos, exponiendo a descargar malware y otras amenazas. Dado que un certificado auto firmado no es "manejado" por una CA, no hay revocación (anular su validez del certificado) en caso de que un atacante robe la clave privada.
R2	El tener una cantidad tan alta de vulnerabilidades críticas en la infraestructura se demuestra que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la Empresa a un ataque.
R3	Un atacante puede hacer un ataque de hombre en el medio explotando la Vulnerabilidad de POODLE, al permitirse SSL v3.0.
R4	Configuraciones y credenciales por defecto en las aplicaciones podrían permitir la Modificación, eliminación o visualización de la información contenida en las bases de datos.
R5	El Contar con vulnerabilidades que datan de hace 8 años o más, demuestran que no existe una gestión continua para tratamiento de vulnerabilidades, exponiendo a la Empresa a un ataque.
R6	Un atacante puede ejecutar un ataque de hombre en el medio aprovechando las múltiples fallas del protocolo criptográfico.
R7	Al comprometer una máquina de usuario, un atacante podría ver todos los servidores y enumerar todos los servicios de cada uno de ellos y explotar aquellos servicios que sean vulnerables.
R8	Cambios a nivel de Sistema operativo o de Aplicación, implementados directamente en ambiente de producción podrían generar indisponibilidad del Sistema de información.

Fuente. Elaborado por los autores.

Cuadro 25. Abreviaturas de controles

Controles	Descripción
C1	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.
C2	Desarrollar Estándares de configuración segura para sistemas operativos, bases de datos, dispositivos de red y aplicaciones.
C3	Cambiar configuraciones por defecto
C4	Desarrollo de la política de controles criptográficos
C5	Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior
C6	Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.
C7	Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).
C8	Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción.
C9	Implementación de entidad certificadora de confianza
C10	Cambiar certificados auto firmados por certificados de confianza

Fuente. Elaborado por los autores.

4.4.3 Reorganización de controles. Los controles se reorganizaron para que su orden estuviese de acuerdo con la criticidad del riesgo abordado como se relaciona en el Cuadro 26. Riesgos vs. controles. En el Cuadro 26. Riesgos vs. controles adicionalmente se puede apreciar que los controles C1 al C10 van solucionando los riesgos del extremo al moderado (no confundir con de R1 a R8 que no están reorganizados por criticidad).

Con esta relación se puede comprender que para reducir los riesgos extremos se deben implementar los controles C1, C2, C3, C4 y C5. Para reducir los Riesgos altos se deben implementar los controles C1, C4, C6, C7 y C8. Y para reducir los riesgos moderados se deben implementar los controles C4, C9 y C10.

Cuadro 26. Riesgos vs. controles

Riesgo vs. controles	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
R1 Moderado				x					X	x
R2 Extremo	x									
R3 Alto				x		x				
R4 Extremo		x	x							
R5 Alto	x									
R6 Extremo				x	x					
R7 Alto							x			
R8 Alto								x		

Fuente. Elaborado por los autores.

4.4.4 Análisis de activos involucrados en los riesgos y los controles. Una vista al cruce de los riesgos presentes contra los activos críticos de TI, dan una noción de cuanto riesgo hay en los activos y en cuales se requerirá más esfuerzo y tiempo para minimizar sus riesgos, para esto se elabora el Cuadro 27. Riesgos sobre activos críticos, con una simple mirada se observa que el activo con mayor cantidad de riesgos es el servidor de base de datos SQL.

Cuadro 27. Riesgos sobre activos críticos

	Activo					
Riesgo	Servidor de aplicación ERP	Servidor de archivos	Servidor de base de datos SQL	Servidor de comunicaciones Asterix - PBX	Servidor de correo electrónico	Servidor de programa de nómina - SARA
R1 Moderado	X	X	X	X	X	X
R2 Extremo	X	X	X	X	X	X
R3 Alto			X			
R4 Extremo			X			
R5 Alto			X			
R6 Extremo				X		
R7 Alto	X	X	X	X	X	X
R8 Alto	X					
TOTAL	4	3	6	4	3	3

Fuente. Elaborado por los autores.

También resulta útil analizar cuáles son los activos en donde se requerirá aplicar mayor cantidad de controles, como se aprecia en el Cuadro 28. Controles vs activos. Esto muestra que el activo que requerirá mayor trabajo es el servidor de base de datos SQL.

Cuadro 28. Controles vs. activos

	Activo					
Control	Servidor de aplicación ERP	Servidor de archivos	Servidor de base de datos SQL	Servidor de comunicaciones Asterix - PBX	Servidor de Correo Electrónico	Servidor de Programa de Nomina - Sara
C1	X	X	X	X	X	X
C2			X			
C3			X			
C4	X	X	X	X	X	X
C5				X		
C6			X			
C7	X	X	X	X	X	X
C8	X					
C9	X	X	X	X	X	X
C10	X	X	X	X	X	X
TOTAL	6	5	8	6	5	5

Fuente. Elaborado por los autores.

4.5 ASPECTOS GENERALES

- Compromiso de la alta gerencia para llevar a cabo el plan de remediación.
- Asignar un responsable en MODANOVA S.A.S para las actividades que aparezcan sin responsable o que no lleguen a ser claras.
- Estudiar la viabilidad financiera.
- Proveer capacitación, asesoría o soporte al responsable interno de las remediaciones y al líder técnico.
- Proveer los recursos necesarios para la implementación de los controles.

4.6 ACTIVIDADES PARA IMPLEMENTAR CONTROLES

4.6.1 Control 1.

4.6.1.1 Descripción. Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.

4.6.1.2 Actividades. Crear comité de administración de parches. Crear al interior de MODANOVA S.A.S un comité para identificar, presentar, sugerir remediaciones, aprobar, permitir, hacer seguimiento y corregir vulnerabilidades de los sistemas de MODANOVA S.A.S.

Este comité estaría conformado por un representante de las principales áreas de la organización, el cual deberá tener el poder de tomar decisiones para el área que represente. Se sugiere que sean los gerentes/directores de las siguientes áreas si existen o se llegara a crear el área: gerencia general, sistemas, bases de datos, servidores, redes, continuidad del negocio, administrativa, financiera, costos, gerencia comercial, recursos humanos, y otra área de importancia para la compañía que utilice activos críticos de T.I**.**

En el comité debe asignarse un líder técnico para hacer seguimiento del progreso de aplicación de las remediaciones de vulnerabilidades, presentar avances y el compilado de parches o cambios a presentar en cada reunión.

Periodicidad de reuniones: Dentro de los 5 primeros días de inicio de cada mes, agendada en común acuerdo entre sus integrantes al finalizar la última reunión. La primera reunión del comité debe ser convocada por la alta gerencia, debe ser de obligatorio cumplimiento y dirigida a las cabezas de áreas mencionadas o seleccionadas por la alta gerencia que harán parte del comité.

Actividades previas a las reuniones. Posterior a la primera reunión del comité, los representantes de las áreas deberán informar al líder técnico del comité con anticipación mínimo de 2 días hábiles, las vulnerabilidades identificadas en sus sistemas, los reléase, parches, actualizaciones, cambios de configuración requeridos para corregir las vulnerabilidades detectadas. Esta información debe presentarse siendo claros en cuales de los sistemas se encuentran presentes, en qué consisten las vulnerabilidades, como se solucionan y en lo posible aportar documentación que respalde esto.

También debe presentarse informe de avances de vulnerabilidades corregidas cuyo compromiso fue adquirido en reuniones previas.

Metodología de las reuniones. Debe haber un encargado de tomar nota de lo discutido en la reunión y elaborar el acta de la misma.

Primera reunión: Presentación del objetivo, justificación, metodología del comité, sus integrantes y responsabilidades, programación de la siguiente reunión.

Reuniones posteriores: El líder técnico presentará los compromisos adquiridos en la reunión previa si se cerró y que se hizo, se reprogramarán aquellos no cerrados o se cerrarán de ser necesarios con observación en el acta y teniendo la aprobación en el comité.

El líder técnico presentará informe de avance en la remediación de vulnerabilidades y observaciones que se den a lugar.

El comité aportará sus observaciones del informe y tomará las decisiones que se den a lugar.

El líder técnico presentará en orden las vulnerabilidades críticas y altas recopiladas a lo largo del mes, los activos que se encontrarían afectados, en que consiste la vulnerabilidad, sus impactos, que hacer para remediarlas y que se requiere, solicitar aprobación del comité para remediarla teniendo en cuenta lo mencionado, establecer un responsable y una fecha prudente para que se encuentre remediada.

Finalizada la reunión a más tardar dos días hábiles después se enviará acta de la misma mediante correo electrónico a los participantes del comité.

Actividad exclusiva del líder técnico. Con la aprobación de la gerencia el líder técnico tendrá que ejecutar semestralmente o anualmente (de acuerdo a como lo

apruebe la gerencia) un análisis de vulnerabilidades técnicas sobre los principales activos críticos de T.I, en caso de no poseer herramienta para ejecutar este análisis se sugiere adquirir una o sub contratar el servicio de análisis de vulnerabilidades. El resultado de este análisis presentará nuevas vulnerabilidades o vulnerabilidades aún no remediadas de las cuales se obtendrá un nuevo insumo para presentar al comité de parches de acuerdo a lo mencionado en la metodología.

Adquirir o utilizar herramienta para distribución de software o actualizaciones. Es necesario contar con una herramienta para distribuir masivamente, silenciosamente y en forma desatendida las actualizaciones en los sistemas informáticos, se recomienda emplear alguna de las siguientes herramientas: WSUS (Windows Server Update Services), Microsoft System Center 2012 o posterior, Symantec Altiris, IBM Tivoli Endpoint Manager (BigFix), Nessus Manager, Red Hat Satellite Server, entre otras.

Los parches, actualizaciones, o cambios de configuraciones que no puedan aplicarse mediante el uso de la herramienta adquirida o no esté soportado mediante la misma deberán ser aplicados manualmente.

4.6.2 Control 2.

4.6.2.1 Descripción. Desarrollar estándares de configuración segura para sistemas operativos, bases de datos, dispositivos de red y aplicaciones.

4.6.2.2 Actividades. Identificación de sistemas y software. Esta sección de la actividad debe ser ejecutada por el líder técnico del proyecto de remediación de riesgos.

Tomar la lista de activos de T.I. previamente aportada en el proyecto y para cada uno de los activos identificados crear una nueva lista de software presente en la misma priorizando en sistemas operativos y los aplicativos citados en el análisis de riesgos.

En los sistemas y aplicativos debe tenerse muy presente las versiones exactas, para los aplicativos que instalan otros productos para sus operaciones o que no tienen variedad de documentación pública, tratar en lo posible de identificar que software adicional se instala o se requiere para su operación.

Descarga de plantillas de configuración segura. Esta actividad debe ser ejecutada por el especialista en seguridad informática asignado al proyecto.

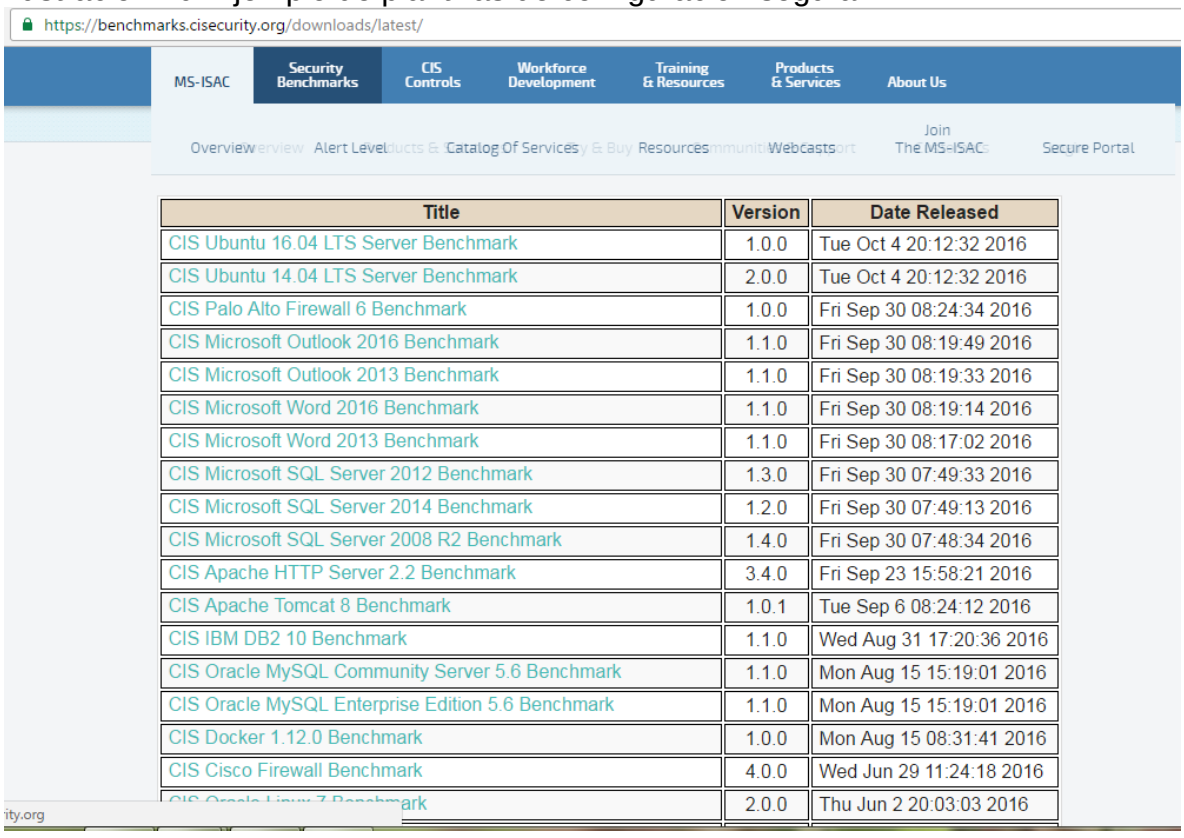
Una vez identificados los productos o software que representen riesgos, se debe proceder a buscar y descargar plantillas de aseguramiento del producto.

Existen diversos sitios en donde se ofrecen plantillas o tutoriales de que puntos deben revisarse en el software, sus vulnerabilidades, amenazas y cómo hacer el aseguramiento.

El principalmente recomendado es:
https://benchmarks.cisecurity.org/downloads/latest/
https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

Un ejemplo del sitio recomendado para descargar plantillas de aseguramiento y un breve vistazo a las plantillas se aprecia en la Ilustración 10. Ejemplo de plantillas de aseguramiento.

Ilustración 10. Ejemplo de plantillas de configuración segura



Title	Version	Date Released
CIS Ubuntu 16.04 LTS Server Benchmark	1.0.0	Tue Oct 4 20:12:32 2016
CIS Ubuntu 14.04 LTS Server Benchmark	2.0.0	Tue Oct 4 20:12:32 2016
CIS Palo Alto Firewall 6 Benchmark	1.0.0	Fri Sep 30 08:24:34 2016
CIS Microsoft Outlook 2016 Benchmark	1.1.0	Fri Sep 30 08:19:49 2016
CIS Microsoft Outlook 2013 Benchmark	1.1.0	Fri Sep 30 08:19:33 2016
CIS Microsoft Word 2016 Benchmark	1.1.0	Fri Sep 30 08:19:14 2016
CIS Microsoft Word 2013 Benchmark	1.1.0	Fri Sep 30 08:17:02 2016
CIS Microsoft SQL Server 2012 Benchmark	1.3.0	Fri Sep 30 07:49:33 2016
CIS Microsoft SQL Server 2014 Benchmark	1.2.0	Fri Sep 30 07:49:13 2016
CIS Microsoft SQL Server 2008 R2 Benchmark	1.4.0	Fri Sep 30 07:48:34 2016
CIS Apache HTTP Server 2.2 Benchmark	3.4.0	Fri Sep 23 15:58:21 2016
CIS Apache Tomcat 8 Benchmark	1.0.1	Tue Sep 6 08:24:12 2016
CIS IBM DB2 10 Benchmark	1.1.0	Wed Aug 31 17:20:36 2016
CIS Oracle MySQL Community Server 5.6 Benchmark	1.1.0	Mon Aug 15 15:19:01 2016
CIS Oracle MySQL Enterprise Edition 5.6 Benchmark	1.1.0	Mon Aug 15 15:19:01 2016
CIS Docker 1.12.0 Benchmark	1.0.0	Mon Aug 15 08:31:41 2016
CIS Cisco Firewall Benchmark	4.0.0	Wed Jun 29 11:24:18 2016
[illegible]	2.0.0	Thu Jun 2 20:03:03 2016

Fuente. https://benchmarks.cisecurity.org

Existen otros sitios que ofrecen también sugerencias para la configuración segura cómo https://www.first.org/resources/guides y

https://security.berkeley.edu/resources/best-practices-how-articles/database-hardening-best-practices
En caso de que no existan plantillas de aseguramiento para el producto a endurecer, se sugiere solicitar al proveedor una plantilla o buenas practicar para asegurar su producto/sistema, en caso negativo por parte del proveedor debe iniciarse una serie de pruebas sobre el software a fin de detectar vulnerabilidades más específicas y con el acompañamiento del especialista en seguridad crear una plantilla propia para el producto.

Elaboración de propuesta de aseguramiento. Esta actividad debe ser ejecutada por el especialista en seguridad informática asignado al proyecto.

Analizada la información del software que posee riesgos y revisadas las platillas de aseguramiento de acuerdo a las versiones reportadas.
Elaborar plantillas Excel de auditoría y aseguramiento para ser aplicadas por el líder técnico.

Evaluación de impactos. No todas las recomendaciones de aseguramiento pueden ser aplicadas en la infraestructura de las empresas, debido a que algunos cambios impactan la operación generando problemas, razón por la cual deben evaluarse en las plantillas de auditoría y aseguramiento que cambios habría que aplicar y sus posibles impactos.

Presentación ante comité de administración de actualizaciones. Tanto las plantillas de auditoría y aseguramiento más los cambios que se requieran hacer en los sistemas, deben ser presentados en el comité de administración de actualizaciones y socializar porque es necesario aplicar cambios, sus beneficios, pero también los posibles impactos de los cambios.

Estos cambios deben ser evaluados cuidadosamente por el comité y autorizados a probar en un ambiente de pruebas.

Implementar en ambiente de pruebas. En caso de que no exista un ambiente de pruebas, se sugiere utilizar otra máquina con características similares al objetivo del aseguramiento y copiar en este el sistema a asegurar, sea por imagen de disco o reinstalando todos los componentes en igual versión y descargando configuraciones del host original para asemejarlo al sistema original.

El objetivo de esta actividad radica en comprobar técnicamente si el cambio puede ser aplicado y observar otros impactos que pudiesen no haber sido anticipados.

Implementar en producción. Si las pruebas en ambiente de desarrollo son exitosas y la plantilla ha sido aprobada en el comité de administración de actualizaciones, se debe proceder a generar copia de seguridad del sistema a asegurar, establecer una ventana de mantenimiento, aplicar la plantilla de aseguramiento y probar que no queden problemas de indisponibilidad o servicios.

Si el resultado de la ventana es satisfactorio debe conservarse la copia de seguridad por lo menos durante un mes mientras se descartan problemas generados en aplicación de la plantilla en producción.

Adicionar plantilla a la línea base del software. Posterior a la aplicación de la plantilla de aseguramiento se debe programar la ejecución de un análisis de vulnerabilidades sobre el servidor asegurado a fin de comprobar la efectividad de la plantilla de aseguramiento, los cambios que corrigieron las vulnerabilidades deben ser tenidos en cuenta en la plantilla para que esta haga parte del documento de línea base para instalación de servidores o software en caso de que exista.

4.6.3 Control 3.

4.6.3.1 Descripción. Cambiar configuraciones por defecto.

4.6.3.2 Actividades. Alinearse con las plantillas de aseguramiento aprobadas. En caso de que ya existan plantillas de aseguramiento aprobadas por MODANOVA S.A.S se procede a revisar las secciones de cambios de configuración y aplicarlas sobre los servidores en donde deba aplicarse este control.

Cambio de configuraciones por defecto. En caso de que para el momento de implementar este control no existan plantillas de aseguramiento para MODANOVA S.A.S, debe procederse a investigar por internet la sección de configuraciones en las plantillas de aseguramiento sugeridas.

Se debe priorizar el esfuerzo en las configuraciones por default y cambiarlas, tales como puertos por default de los servicios, nombres de usuario, anuncio de banners de configuración, etc.

Paso por comité de administración de actualizaciones, ambiente de pruebas y producción. Al igual que como en el control2, este cambio debe evaluarse en la misma forma en el comité de administración de actualizaciones, ser probado cuidadosamente en ambiente de pruebas y pasar a producción como se establece en el control2.

4.6.4 Control 4.

4.6.4.1 Descripción. Desarrollo de la política de controles criptográficos.

4.6.4.2 Actividades. **Desarrollo de política de controles criptográficos.** Una organización alineada con metodologías de seguridad de la información o que pretendan cumplir con estándares de seguridad, lo mínimo que debe tener es una política de controles criptográficos; por tal motivo se presenta una propuesta de política de controles criptográficos, la cual puede ser alterada o mejorada de acuerdo al nivel de seguridad que desee MODANOVA S.A.S o expandir su alcance.

Política propuesta. *"Todos los activos de información de T.I catalogados como críticos y que utilicen algún sistema criptográfico sea cliente o servidor, debe someterse a la política de controles criptográficos.*

Toda información catalogada como reservada, altamente sensible o crítica deberá cifrarse al momento de almacenarse o transmitirse por cualquier medio.

El responsable de aplicar la política de controles criptográficos es el jefe de sistemas.

El jefe de sistemas debe desarrollar y establecer estándares y procedimientos para el uso de controles criptográficos, basados en el mejor algoritmo criptográfico posible que genere el menor impacto en las operaciones del negocio y que proporcione un alto nivel de seguridad en la protección de la información.

El jefe de sistemas será responsable de desarrollar y establecer el proceso de generación, administración, custodia, protección, mecanismos de distribución, recuperación de llaves criptográficas, tratamiento de llaves comprometidas, destrucción y cualquier otra actividad relacionada con el manejo de llaves criptográficas. Cuando las llaves privadas se entregan a usuarios finales la responsabilidad de protección recae sobre quien la recibe.

Toda información que se vaya a cifrar debe haber sido primero analizada por software antivirus con firmas actualizadas.

Es responsabilidad de quien usa la información indicar al jefe de sistemas (quien la almacena o proporciona los medios para transferirla) cuando una información es sensible, reservada o crítica y necesita protección mediante cifrado."

4.6.5 Control 5

4.6.5.1 Descripción. Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior.

4.6.5.2 Actividades. **Actualización de navegadores y sistemas operativos.** A versiones inferiores de internet Explorer 9 no se les puede activar TLS 1.1 por lo cual se hace necesario actualizar el software navegador a última versión estable aprobada por MODANOVA S.A.S siempre y cuando se pueda instalar Internet Explorer 9 o superior en el sistema operativo, de lo contrario habría que actualizar el sistema operativo a última versión estable. Vale la pena recordar que en sistemas operativos Microsoft inferiores a Windows 7 no se puede usar TLS 1.1 o 1.2.

Se debe restringir el uso de otros navegadores en los que no se pueda deshabilitar SSL 2.0, 3.0 y activar TLS 1.1 o superior.

El procedimiento técnico para realizar esta actividad está descrito en el enlace: https://help.salesforce.com/apex/HTViewSolution?urlname=Enabling-TLS-1-1-and-TLS-1-2-in-Internet-Explorer&siteLang=es

Política de dominio. Una forma sencilla y masiva para cambiar la configuración del navegador internet Explorer es mediante el uso de una política de dominio que cambie dicha configuración, no obstante, no aplica en navegadores incompatibles y navegadores diferentes a Microsoft Internet Explorer.

El procedimiento técnico para realizar esta está descrito en el enlace: http://www.bauer-power.net/2014/06/how-to-enabled-tls-11-and-tls-12-in.html#.WBZLPdXhDIU

4.6.6 Control 6

4.6.6.1 Descripción. Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.

4.6.6.2 Actividades. **Desactivar SSL 3.0 o inferior en servidores y habilitar TLS 1.1 o superior.** El procedimiento técnico de activación de TLS 1.1 o superior y deshabilitado de SSL inferior o igual a 3.0 para Servidores Microsoft e IIS, esta descrito en el siguiente enlace: http://tecadmin.net/enable-tls-on-windows-server-and-iis/#

El procedimiento técnico de activación de TLS 1.1 o superior y deshabilitado de SSL inferior o igual a 3.0 para Servidores Web diferentes a Microsoft, esta descrito en el siguiente enlace:

https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/

Actualización de navegadores y sistemas operativos. A versiones inferiores de internet Explorer 9 no se les puede activar TLS 1.1 por lo cual se hace necesario actualizar el software navegador a última versión estable aprobada por MODANOVA S.A.S siempre y cuando se pueda instalar internet Explorer 9 o superior en el sistema operativo, de lo contrario habría que actualizar el sistema operativo a última versión estable. Vale la pena recordar que en sistemas operativos Microsoft inferiores a Windows 7 no se puede usar TLS 1.1 o 1.2.

Se debe restringir el uso de otros navegadores en los que no se pueda deshabilitar SSL 2.0, 3.0 y activar TLS 1.1 o superior.
El procedimiento técnico para realizar esta actividad está descrito en el enlace:
https://help.salesforce.com/apex/HTViewSolution?urlname=Enabling-TLS-1-1-and-TLS-1-2-in-Internet-Explorer&siteLang=es

Política de dominio. Una forma sencilla y masiva para cambiar la configuración del navegador internet Explorer es mediante el uso de una política de dominio que cambie dicha configuración, no obstante, no aplica en navegadores incompatibles y navegadores diferentes a Microsoft Internet Explorer.

El procedimiento técnico para realizar esta está descrito en el enlace:
http://www.bauer-power.net/2014/06/how-to-enabled-tls-11-and-tls-12-in.html#.WBZLPdXhDIU

4.6.7 Control 7

4.6.7.1 Descripción. Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).

4.6.7.2 Actividades. **Identificar áreas, zonas y equipos.** Proceder a documentar los equipos conectados a la red de la sede administrativa de MODANOVA S.A.S., sus IP actuales, *hostname*, tipo de equipo, función, ubicación física, área a que pertenece, zona y cualquier otra información que resulte útil como por ejemplo si el punto de red tiene una marca o nomenclatura especial.

Definir criterio para segmentación. Dado que el alcance del proyecto en que se basa el presente plan de trabajo está limitado a los activos críticos de T.I. de la sede administrativa de MODANOVA S.A.S. se sugiere que la segmentación sea realizada por áreas funcionales, ejemplo: Servidores, Contabilidad, Administrativa, Gerencias, recursos humanos, etc.

Aunque para el proyecto los activos críticos de T.I. son los servidores, se recomienda que para la segmentación se expanda un poco más el alcance para incluir equipos que interactúen con el área de servidores.

Se recomienda que las áreas de gerencias no estén dentro de la misma VLAN de los demás equipos de su gerencia debido a que estas máquinas se rigen por distintas políticas a las de servidores y usuarios comunes.

Contabilizar segmentos y equipos. Una vez hecho el inventario de dispositivos proceder a analizar la información y documentar cuales son las áreas funcionales y cuantos dispositivos se encuentran conectados a la misma.

Definir rango de direcciones IP, redes y VLAN. Con el análisis de las áreas identificadas y sus dispositivos, proceder a crear una tabla de segmentos de red en donde se sugiere asignar por área direcciones IP privadas de clase A, como por ejemplo redes 10.0.0.0, 10.0.1.0, con máscara 24 o más pequeña dependiendo de la cantidad de equipos a incluir y manteniendo una holgura para crecimiento, etc.

Asignar direcciones IP a los dispositivos de acuerdo a la red a que pertenezcan y definir un nombre para las VLAN de las redes. De esta forma pueden existir hasta 255 redes con un máximo de 255 IP.

Cambiar direccionamiento IP. Programar actividad para cambiar las direcciones IP de los dispositivos o equipos de acuerdo al rango establecido en el punto anterior.

Asignar switch para crear las VLAN. Para llevar a cabo la creación de VLAN se requiere utilizar un switch capa 3 con cantidad de puertos disponibles mayor o igual a la cantidad de redes o VLAN a crear.

Establecer puertos a asignar. De acuerdo a como se definan las redes a asociar por VLAN se debe definir y etiquetar en el switch de capa 3 que puerto corresponde a que VLAN.

Cambiar cableado en switch. El cableado que debe estar debidamente etiquetado e identificado, debe permitir saber a qué área, red o VLAN pertenece dicho punto y reconectarlo a un switch de capa 2 para asignar a dicha VLAN y este a su vez conectarse al puerto del switch capa 3 que corresponde a la VLAN.

Crear VLAN’s. En el switch de capa 3 asignado para crear las VLAN proceder a asignar y configurar un puerto a cada una de las VLAN a crear y etiquetarlos, se

pueden utilizar los switches de capa 2 para conectar las diferentes redes al puerto correspondiente de VLAN en el switch capa 3.

Actualizar DNS. Proceder a actualizar en el servidor DNS las nuevas direcciones IP de los servidores.

Crear listas de control de Acceso ACL. Crear las listas de control de acceso en las tablas de enrutamiento de cada uno de los switch que comunican a cada una de las redes de las diferentes áreas, con el fin que solo se permita el tráfico permitido para cada una.

4.6.8 Control 8

4.6.8.1 Descripción. Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción.

4.6.8.2 Recursos. Mínimo 6 servidores, con características físicas lo más similares posibles a los activos críticos de T.I. identificados en el proyecto, pero con copia idéntica (preferiblemente imagen) del sistema operativo, software, aplicaciones, configuraciones y datos de producción.

4.6.8.3 Actividades. **Nueva red o VLAN.** Se recomienda crear una nueva red o VLAN para contener equipos de pruebas.

Máquinas para la nueva red o VLAN. Dado que los activos de T.I. críticos son los seis servidores de la siguiente lista:

- Servidor De Aplicación ERP
- Servidor de Archivos
- Servidor De Base De Datos SQL
- Servidor de comunicaciones Asterix - PBX
- Servidor de Correo Electrónico
- Servidor de Programa de Nomina – Sara

Se adquirirán o asignarán estos nuevos servidores tendrán características físicas lo más similares posibles a los reales, pero con copia idéntica (preferiblemente imagen) del sistema operativo, software, aplicaciones, configuraciones y datos de producción.

Estos nuevos servidores serán ingresados en la nueva red o VLAN de pruebas.

Cambios particulares sobre los servidores de este ambiente. Una vez ingresados los servidores en el ambiente de pruebas se debe proceder a cambiar su direccionamiento IP y cambiarle el *hostname*.

Restricciones y auditorias. Estos servidores en el ambiente de pruebas que contienen datos de ambiente productivo deben estar sometidos a las mismas o mayor cantidad de políticas de seguridad que en producción.

Se debe restringir el acceso a estas máquinas mediante listas de acceso de firewall, registrar y auditar toda actividad relacionada con estos servidores.

4.6.9 Control 9

4.6.9.1 Descripción. Implementación de entidad certificadora de confianza.

4.6.9.2 Recursos.1 Servidor que soporte Windows Server 2012
1 Licencia de Windows Server 2012

4.6.9.3 Actividades. **Instalar sistema operativo que pueda brindar servicios de CA (Entidad Certificadora).** Instalar el sistema operativo Windows Server 2012 en el nuevo servidor y cargar la licencia adquirida para el mismo.

Agregar role de entidad certificadora. Agregar en las características de software el role “Active Directory Certificate Services” e instalar la herramienta “Certification Authority Management Tools”.

Configurar el role para convertir el equipo en una entidad certificadora del tipo root y configurar sus parámetros de acuerdo a la política de controles criptográficos definida en el control 4.

Asegurar la nueva llave privada. Crear la llave privada y almacenarla en un lugar seguro de acuerdo a la política de controles criptográficos.

En caso de que no se haya definido los estándares de la política de controles criptográficos, se sugiere como se use el algoritmo SHA256 con longitud 2048.
El procedimiento técnico se encuentra especificado paso a paso en el hipervínculo: https://windowserver.wordpress.com/2013/04/12/windows-server-2012-instalando-una-autoridad-certificadora-raz-root-certification-authority-de-tipo-standalone/

4.6.10 Control 10

4.6.10.1 Descripción. Cambiar certificados auto firmados por certificados de confianza.

4.6.10.2 Actividades. Para ejecutar este control es necesario tener una entidad certificadora sea una propia como la que se implementa en el control 9 o comprar certificados digitales en entidades como Verisign.

Opción de compra de certificados. El costo aproximado de cada certificado comprado sería de $6 USD aproximadamente por un año.
Se deben seguir las instrucciones de la compañía que vende estos certificados.
Opción de certificado con CA propia. Generar CSR, Los aplicativos que estén utilizando certificados autofirmados y requieran este certificado emitido por una entidad de confianza deben hacer un CSR (Certificate Signing Request / Solicitud de Firmar un Certificado).

Se deben diligenciar los campos solicitados en el CSR.

Procedimientos técnicos para generar un CSR:
https://www.digicert.com/es/crear-csr.htm

Entregar archivo CSR al administrador de la CA (Entidad Certificadora). El administrador de la CA entregará un nuevo certificado digital al solicitante el cual deberá ser instalado en el servidor web que lo necesita.

4.7 RIESGO RESIDUAL

Una vez realizada la implementación de los controles recomendados en su orden de valoración para impacto vs probabilidad, se estima que los riesgos encontrados se puedan reducir de la siguiente forma:

- Los riesgos R2, R4 y R6 de carácter extremo, al aplicar los controles recomendados se estima que estos riesgos se reduzcan hasta el nivel moderado, identificado con el color azul.

- Los riesgos R3, R5, R7 y R8 de carácter alto, al aplicar los controles recomendados se estima que estos riesgos se reduzcan hasta el nivel bajo identificado con el color verde.

- El riesgo R1 de carácter moderado, al aplicar los controles recomendados se estima que este riesgo se mantenga en el nivel más bajo (bajo) identificado con el color verde.

El Cuadro 29. Riesgos residuales, presenta en forma agrupada como se estima que quedarían los riesgos residuales una vez implementados los controles.

Cuadro 29. Riesgos residuales

Combinaciones de riesgo	**Impacto**				
Probabilidad	Inferior	Menor	Importante	Mayor	Superior
Muy alta					
Alta					
Moderada	2	3			
Baja		2			
Muy baja	1				

Fuente Elaborado por los autores

Hay que aclarar que estos valores son estimados pues los valores reales se deben calcular una vez se haya realizado la implementación del plan de trabajo recomendado y se terminen todas las tareas que allí se mencionan, teniendo en cuenta el supuesto de que la empresa realice todas las actividades al 100%, pues es decisión de MODANOVA S.A.S. realizar estas actividades.

La única forma de eliminar completamente un riesgo es retirar el activo o los activos afectados, razón por la cual siempre existirán riesgos.

4.8 COSTOS Y DURACIÓN ESTIMADA

Los costos que se detallan a continuación se estiman basados en que MODANOVA S.A.S. utilizará personal interno para llevar a cabo la mayor parte de las actividades excepto aquellas que requieren compra de hardware, software o servicios asumiendo que no contratará personal especializado.

La duración se basa en que las actividades no son ejecutadas en forma paralela y que son ejecutadas en su mayoría por personal interno de MODANOVA S.A.S.

El detalle acerca del control a implementar, su duración y costo se estima en el Cuadro 30. Costos estimados.

Cuadro 30. Costos estimados

Control	Descripción	Duración estimada para implementación	Costo estimado de hardware, software y servicios contratados
Control 1	Desarrollar un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.	1 mes	$ 500.000
Control 2	Desarrollar Estándares de configuración segura (hardening) para sistemas operativos, bases de datos, dispositivos de red y aplicaciones.	6 meses	$3.000.000
Control 3	Cambiar configuraciones por defecto.	4 meses	$ 500.000
Control 4	Desarrollo de la política de controles criptográficos.	1 Semana	$ 300.000
Control 5	Deshabilitar el protocolo SSL 2.0 y 3.0, para emplear TLS 1.1 o superior.	2 Meses	$ 450.000
Control 6	Deshabilitar el protocolo SSL 3.0 en los clientes, en el servidor o en ambos.	3 Meses	$ 550.000
Control 7	Segmentar la red en VLAN's y entre las diferentes VLAN's establecer listas de control de acceso (ACL).	3 Meses	$ 1.200.000
Control 8	Desarrollar un ambiente de pruebas que permita testear los cambios antes de ser aplicados en ambiente de producción.	6 meses	$60.000.000
Control 9	Implementación de entidad certificadora de confianza.	2 meses	$12.000.000
Control 10	Cambiar certificados auto firmados por certificados de confianza.	3 meses	$120.000
TOTAL			**$78.620.000**

Fuente. Elaborado por los autores.

5. CONCLUSIONES

El análisis de riesgos es una actividad muy útil al momento de querer conocer en que tanto peligro se encuentra o que propensa es a ser afectada una organización, que proteger, como hacerlo y que sucedería “si”. Por lo anterior resulta muy útil desarrollar metodologías para realizar estos análisis que normalmente son lineamientos y dicen evalúen activos, definan criticidades, establezcan controles, etc.; pero no se suelen indicar con ejemplos o decir el cómo hacer las cosas, esto suele confundir a estudiantes que están aprendiendo a hacer análisis de riesgos y gracias al desarrollo de este proyecto se obtiene una guía con metodología, elaboración de matrices para el levantamiento de información, definición de niveles de probabilidad, impacto, criticidades, etc. y propuesta de controles para mitigar riesgos basados en la norma ISO 27001 que puede ser utilizado como guía para futuros análisis de riesgos en activos de T.I.

Se pensaron en varios estándares de seguridad de la información como COBIT, Information Security Forum's Standard of Good Practice" (SOGP), Information Security Management Maturity Model ("ISM3") e ISO/IEC 27001:2013 y finalmente se escogió ISO 27001 sobre las demás para este proyecto, debido a que es el estándar más popular para implementar sistemas de seguridad de la información y está estrechamente ligada con la ISO 27002 que en resumen son estándares de seguridad que proveen controles, además como MODANOVA S.A.S. pretende en un futuro no muy lejano obtener certificaciones de calidad, lo más adecuado es alinearse con los estándares más importantes y útiles en Colombia como lo son los estándares ISO.

Durante el desarrollo del presente proyecto se realizó un inventario de activos de T.I., funciones de los mismos y definir criticidades, lo cual no existía en MODANOVA S.A.S., tener este estudio y la clasificación de los mismos otorga a la compañía un foco de activos que deben proteger o priorizar, además de que es necesario tener esto para poder obtener certificaciones como ISO9001 e ISO27001.

La formulación del problema de este proyecto fue solucionada aplicando la metodología de ISO 27001 e ISO 27005, pero obligando a diseñar formatos, Cuadros de clasificación, valoraciones, ponderaciones, métodos para hacer un buen análisis de la información, diseños de controles y cómo implementarlos. Como resultado se generó nuevo conocimiento que será de gran utilidad para estudiantes, profesionales de seguridad informática/ de la información y principalmente para MODANOVA S.A.S.

Todo el proyecto fue basado en las normas ISO/IEC 27001, ISO/IEC 27002, e ISO/IEC 27005, las cuales fueron de gran ayuda para realizar los pasos recomendados para obtener una evaluación correcta de cada uno de los activos, la mejor forma de lograr las respectivas correcciones y mejoras sobre cada uno de los sistemas. Se demuestra que estas normas no dan la solución a todos los problemas de seguridad, pero efectivamente son de las mejores metodologías para abordar los puntos más importantes y conseguir los resultados deseados.

De igual forma se puede concluir que estas normas están realizadas de forma que pueden ser aplicadas a cualquier tipo de empresa, grande o pequeña la cual requiera una administración adecuada de sus activos informáticos bajo los estándares que se manejan en la industria.

Gracias al desarrollo de este proyecto hubo la necesidad de inventariar los activos de T.I. y evaluar sus criticidades, esto aportó un mapa claro de que activos de T.I. son los más críticos para la empresa y en donde debe hacer esfuerzos para proteger la información. Además, este será insumo para nuevos análisis de vulnerabilidades y de riesgos.

Los riesgos identificados en MODANOVA S.A.S. invitan a reflexionar en que en muchas otras empresas de Colombia que, aunque también han crecido y nunca antes han pensado en seguridad informática, pero que utilizan la tecnología para apoyar los procesos misionales; no saben el riesgo y el peligro al que están expuestas, y es aquí donde los profesionales en seguridad son invitados a proteger las empresas, las personas y promover la cultura de la seguridad en el país.

Adicionalmente también se puede concluir que la implementación de políticas de seguridad informáticas en una organización es una solución que no sólo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización.

Es por esto que preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada, es una de las principales metas de esta estrategia.

Los riesgos identificados han demostrado serias falencias de seguridad en los activos críticos de T.I. tanto así que se identificaron 8 riesgos, de los cuales tres son extremos, cuatro altos y uno moderado. Riesgos que muy probablemente han de

comprometer la información, los sistemas de MODANOVA S.A.S. y que son de fácil explotación. De llegarse a materializar alguno de estos riesgos MODANOVA S.A.S. se verá en serios problemas, dado el alto impacto de los mismos y le será muy difícil recuperarse dada la ausencia de controles específicos.

Se evidencia claramente que MODANOVA S.A.S. tiene grandes falencias en seguridad las cuales no habían sido vistas debido a la ausencia de un área de seguridad y desconocimiento de la importancia de la seguridad informática por parte de la gerencia y del área de sistemas. El riesgo existente y sus impactos también eran desconocidos para MODANOVA S.A.S.

Con los resultados de este proyecto MODANOVA S.A.S. podrá iniciar la primera etapa de evaluar que riesgos expuestos se van a tratar, la viabilidad de la implementación de los controles propuestos y sus costos. Con esto dicho ya se puede solicitar, elaborar o aprobar planes de trabajo para la implementación de los controles propuestos y así minimizar los riesgos identificados.

MODANOVA S.A. no se encuentra preparada para iniciar un proceso de certificación en ISO 9001 o ISO27001 dada las falencias encontradas en el presente análisis y la carencia de un área de seguridad.

El proceso ejecutado en este proyecto podría mejorarse si se extendiera su alcance más allá de los activos críticos de T.I. ya que hay más activos, procesos y personas involucrados, que pueden ser foco de ataques o daños a la infraestructura y la información. Como por ejemplo el acceso a las instalaciones, estaciones de trabajo e incluso la misma carencia del área de seguridad permitirá la existencia de nuevos riesgos, cómo que se debe hacer ante un incidente de seguridad que comprometa el patrimonio de la compañía.

Hacer uso de mayor variedad de herramientas de análisis de vulnerabilidades, Hacking Ético e ingeniería social pueden aportar nuevas vulnerabilidades y riesgos no contemplados.

6. RECOMENDACIONES

Socializar con la alta gerencia y el área de sistemas de T.I. los riesgos encontrados en el presente proyecto y que se acuerden compromisos para aplicar las acciones de control recomendadas en los apartados citados en el presente proyecto “Tratamiento del riesgo“ y “Plan de trabajo para implementar los controles”.

Para el presente proyecto se desarrolló un capítulo que va más allá del alcance establecido y contempla pautas que permitirán a MODANOVA S.A.S. iniciar la implementación de los controles propuestos en este proyecto, el capítulo 4 “PLAN DE TRABAJO PARA IMPLEMENTAR LOS CONTROLES”. Se recomienda que este plan de trabajo propuesto sea evaluado por la alta gerencia en compañía del jefe de sistemas de la misma a fin de tomar la decisión de que riesgos abordar, que controles implementar y la viabilidad de los mismos.

El área de sistemas o un tercero se encargue de proponer a la alta gerencia y el área de sistemas un plan específico para llevar a cabo las acciones de control recomendadas en el presente proyecto o mejorar el plan propuesto.

Que la alta gerencia apruebe un presupuesto y sobre que riesgos desea actuar, aprobar ejecución del plan para reducción del riesgo informático sobre los activos críticos de T.I.

Realizar un nuevo análisis de riesgos una vez ejecutado del plan para reducción del riesgo informático sobre los activos críticos de T.I., calcular el riesgo residual y trabajar sobre las políticas de tratamiento.

Implementar un plan de revisiones periódicas 1 o 2 veces al año con el fin de evaluar el estado de los riesgos basados en los últimos hallazgos que se tengan, de reportes anteriores y ver si se ha generado algún nuevo riesgo, desarrollando un procedimiento formal, sistemático y repetible, para la identificación, el seguimiento, control, atención y cierre de vulnerabilidades técnicas.

Tratar en lo posible de intentar mitigar los riesgos de acuerdo con sus severidades, primero extremo, luego alto y por último moderado.

Que la alta gerencia apruebe el presupuesto necesario para implementar los controles de los riesgos a tratar.

Implementar los controles aprobados que se propusieron en el presente proyecto siguiendo el plan de trabajo para implementar los controles.

Crear un área de seguridad y contratar o promover a un ingeniero con características idóneas para ejercer el cargo de oficial / director / jefe de seguridad informática / de la información.

Adquirir e implementar una herramienta líder en el mercado para detección de vulnerabilidades.

Capacitar al personal de la compañía es primordial debido a que éste puede tomar un papel activo dentro de la organización de manera que aplique este conocimiento en las diversas actividades que realiza dentro y fuera de la organización con el propósito de proteger de una forma adecuada la información que se les confía, así como la propia.

BIBLIOGRAFÍA

COBIT. ISACA Trust in, and value from, information systems. [en línea] https://www.isaca.org/Pages/default.aspx. Marco de referencia para optimizar y salvaguardas los recursos o activos de información y tecnológicos de cualquier empresa.

Erb, Markus. (2014). Seguridad de la Información y Protección de Datos. Protegete.Wordpress.com: Gestión de Riesgo en la Seguridad Informática. [en línea]. http://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion

Giovanni Zuccardi, Juan David Gutiérrez, ISO-27001:2005, En que consiste 27001-Evolución del estándar-Familia 2700x, septiembre de 2006[en línea]. http://pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001v0.1.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Normas Colombianas para la presentación de trabajos de investigación. Sexta Actualización, Santa Fe De Bogotá. ICONTEC, 2008, NTC 1486.

ISO (2005). Gestión de la seguridad de la información. Norma ISO / IEC 27001.

Ley 1273 de 2009. Ministerio de Tecnologías de la Información y de las Telecomunicaciones (Min TIC). [en línea]. http://www.mintic.gov.co/portal/604/w3-article-3705.html

Ley estatutaria 1581 de 2012. Decreto 1377 de 2013. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. (octubre 17) [en línea]. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

PHVA ¿Qué es el ciclo PHVA? Enero 09 de 2010. Blog de Seguridad informática. [en línea]. http://securityjeifer.wordpress.com/tag/phva/. Conceptos enmarcados sobre la ejecución de este ciclo útil dentro de los procesos (sistemas) de gestión de la calidad, incluyendo los de seguridad de la información.

ANEXOS

Anexo A. Constancia de ejecución del proyecto

Modanova s.a.s.
NIT.: 800.161.656-3
Cra. 62 No. 10 - 40
PBX: 745 8800 • Fax: Ext. 318
Bogotá, D.C. - Colombia
E-mail: modanova@modanova.com.co

Bogotá D.C., 22 de noviembre de 2016

Señores:
UNIVERSIDAD PILOTO DE COLOMBIA
Ciudad.

MODANOVA S.A.S.

Hace constar que:

Los estudiantes de la Universidad Piloto de Colombia **FERNANDO CASTIBLANCO** y **LUIS ALEXANDER OVIEDO REGUEROS** identificados con cédula de ciudanía No. 80.471.074 y 7.572.488 respectivamente, desarrollaron en la sede administrativa de MODANOVA S.A.S. y para MODANOVA S.A.S. el proyecto de grado titulado "**ANÁLISIS DE RIESGOS INFORMÁTICOS Y SUGERENCIA DE CONTROLES PARA LA MITIGACIÓN DEL RIESGO EMPLEANDO LAS NORMAS ISO/IEC 27001, ISO/IEC 27002 ISO/IEC 27005 SOBRE LOS ACTIVOS CRÍTICOS DE T.I. EN LA SEDE ADMINISTRATIVA DE LA EMPRESA MODANOVA S.A.S.**"

Los estudiantes desarrollaron su proyecto sobre los activos del área de tecnología en la sede administrativa de MODANOVA S.A.S, con el fin de detectar riesgos de tipo tecnológico y elaborar un plan de mejora para los mismos.

Este proyecto fue realizado en su totalidad bajo la autorización de la gerencia general de **MODANOVA S.A.S**, siendo este proyecto un gran aporte para la compañía en cuanto a seguridad informática se refiere, quedando ahora en manos **MODANOVA S.A.S**. realizar las actividades de remediación del plan de trabajo y estudiar la viabilidad de aplicar las recomendaciones.

Para constancia de firma a los 22 días del mes de noviembre del 2016.

MODANOVA S.A.S.
NIT.: 800.161.656-3

YANZABETH DEL VALLE SAMPER
Gerente General
Modanova S.A.S.

Anexo B. Reportes de nessus

REPORTES DE NESSUS

Nessus Scan Report

Tue, 12 Jul 2016 20:54:27 GMT-0500

Table Of Contents

[-] Collapse All

[+] Expand All

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	1	29	36

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure

Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection

Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	72779	DNS Server Version Detection
Info	72780	Microsoft DNS Server Version Detection
Info	84047	Hyper-V Virtual Machine Detection
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm

Summary

Critical	High	Medium	Low	Info	Total
3	6	12	3	48	72

Details

Severity	Plugin Id	Name
Critical (10.0)	85181	HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE)
Critical (10.0)	90150	HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam)
Critical (10.0)	91222	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)
High (9.7)	59851	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities
High (9.3)	66541	HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution

High (9.3)	76345	HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities
High (9.0)	70118	HP System Management Homepage ginkgosnmp.inc Command Injection
High (7.8)	69020	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities (BEAST)
High (7.5)	90251	HP System Management Homepage < 7.2.6 Multiple Vulnerabilities (FREAK)
Medium (6.8)	72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.8)	50686	IP Forwarding Enabled
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10144	Microsoft SQL Server TCP/IP Listener Detection
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10622	PPTP Detection
Info	10674	Microsoft SQL Server UDP Query Remote Version Disclosure
Info	10736	DCE Services Enumeration
Info	10746	HP System Management Homepage Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43829	Kerberos Information Disclosure
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
Info	64814	Terminal Services Use SSL/TLS
Info	66173	RDP Screenshot
Info	66334	patch Report
Info	69482	Microsoft SQL Server STARTTLS Support

Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	72779	DNS Server Version Detection
Info	72780	Microsoft DNS Server Version Detection
Info	84047	Hyper-V Virtual Machine Detection
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	35	41

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information

Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported

Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	72779	DNS Server Version Detection
Info	72780	Microsoft DNS Server Version Detection
Info	84047	Hyper-V Virtual Machine Detection
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm

Summary

Critical	High	Medium	Low	Info	Total
0	0	11	3	38	52

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	56983	SIP Username Enumeration
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure

Medium (4.3)	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	90317	SSH Weak Algorithms Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10386	Web Server No 404 Error Code Check
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	14773	Service Detection: 3 ASCII Digit Code Responses
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20834	Inter-Asterisk eXchange Protocol Detection
Info	21642	Session Initiation Protocol Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection

Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security patch Detection (SSH)
Info	39521	Backported Security patch Detection (WWW)
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	51891	SSL Session Resume Supported
Info	53360	SSL Server Accepts Weak Diffie-Hellman Keys
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	63202	Asterisk Detection
Info	66334	patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	70657	SSH Algorithms and Languages Supported
Info	76347	HylaFAX Installed
Info	84502	HSTS Missing From HTTPS Server
Info	84574	Backported Security patch Detection (PHP)

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	5	35	43

Details

Severity	Plugin Id	Name
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Low (2.6)	91572	OpenSSL AES-NI Padding Oracle MitM Information Disclosure
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection
Info	10263	SMTP Server Detection
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11414	IMAP Service Banner Retrieval
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	20870	LDAP Server Detection

Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	35716	Ethernet Card Manufacturer Detection
Info	42085	IMAP Service STARTTLS Command Support
Info	42087	POP3 Service STLS Command Support
Info	42088	SMTP Service STARTTLS Command Support
Info	42329	LDAP Service STARTTLS Command Support
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	54580	SMTP Authentication Methods
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	66334	patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	72584	Zimbra Collaboration Server Web Detection
Info	84502	HSTS Missing From HTTPS Server

Summary

Critical	High	Medium	Low	Info	Total

0	0	3	1	34	38

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10919	Open Port Re-check
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11936	OS Identification

Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	15588	Web Server SSL Port HTTP Traffic Detection
Info	19506	Nessus Scan Information
Info	20870	LDAP Server Detection
Info	22964	Service Detection
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry: Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	43829	Kerberos Information Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	64814	Terminal Services Use SSL/TLS
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm